

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
30 January 2003 (30.01.2003)

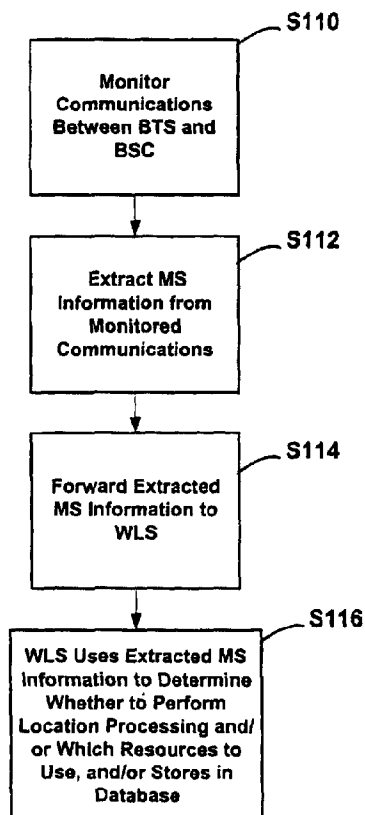
PCT

(10) International Publication Number
WO 03/009612 A1

- (51) International Patent Classification⁷: **H04Q 7/20** (74) Agent: **STEIN, Michael, D.**; Woodcock Washburn LLP, 46th Floor, One Liberty Place, Philadelphia, PA 19103 (US).
- (21) International Application Number: PCT/US02/22390
- (22) International Filing Date: 15 July 2002 (15.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/909,221 18 July 2001 (18.07.2001) US
- (71) Applicant (for all designated States except US): **TRUE-POSITION, INC.** [US/US]; 780 Fifth Avenue, King of Prussia, PA 19406 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **ANDERSON, Robert, J.** [US/US]; 704 Deer Run, Norristown, PA 19403 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GI, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,

[Continued on next page]

(54) Title: MONITORING OF CALL INFORMATION IN A WIRELESS LOCATION SYSTEM



(57) Abstract: In an overlay Wireless Location System, an Abis interface is monitored to obtain information used to locate GSM phones (S116). Signaling links of the Abis interface are passively monitored to obtain certain information, such as control and traffic channel assignment, called number, and mobile identification, which is not available from the GSM air interface of the reverse channel (S110-S116). This approach also applies to IDEN and can be broadened to include CDMA systems where the GSM architecture has been used and the system includes a separated BTS to BSC interface.

WO 03/009612 A1



TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

MONITORING OF CALL INFORMATION IN A WIRELESS LOCATION SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

5 This is a continuation-in-part of U.S. Patent Application Serial No. 09/539,352, filed March 31, 2000, "Centralized Database for a Wireless Location System," which is a continuation of U.S. Patent Application Serial No. 09/227,764, filed January 8, 1999, now U.S. Patent No. 6,184,829 B1, Feb. 6, 2001, "Calibration for Wireless Location System."

10

FIELD OF THE INVENTION

 The present invention relates generally to methods and apparatus for locating wireless transmitters, such as those used in analog or digital cellular systems, personal communications systems (PCS), enhanced specialized mobile radios (ESMRs), and other
15 types of wireless communications systems. More particularly, the present invention relates to the collection of call information from the wireless network's non-air interfaces to facilitate location via TDOA, AOA, and/or TDOA/AOA hybrid wireless location systems in wireless systems having a separated Base Transceiver Station (BTS) and Base Station Controller (BSC).

20

BACKGROUND OF THE INVENTION

 Early work relating to Wireless Location Systems is described in U.S. Patent Number 5,327,144, July 5, 1994, "Cellular Telephone Location System," which discloses a system for locating cellular telephones using novel time difference of arrival (TDOA)
25 techniques. Further enhancements of the system disclosed in the '144 patent are disclosed in U.S. Patent Number 5,608,410, March 4, 1997, "System for Locating a Source of Bursty Transmissions." Both of these patents are assigned to TruePosition, Inc., the assignee of the present invention, and both are incorporated herein by reference. TruePosition has continued to develop significant enhancements to the original inventive
30 concepts and have developed techniques to further improve the accuracy of Wireless Location Systems while significantly reducing the cost of these systems. Patents relating to such enhancements include, but are not necessarily limited to: U.S. Patent No.

6,091,362, July 18, 2000, "Bandwidth Synthesis for Wireless Location System"; U.S. Patent No. 6,097,336, August 1, 2000, "Method for Improving the Accuracy of a Wireless Location System"; U.S. Patent No. 6,115,599, September 5, 2000, "Directed Retry Method for Use in a Wireless Location System"; U.S. Patent No. 6,172,644 B1, 5 January 9, 2001, "Emergency Location Method for a Wireless Location System"; and U.S. Patent No. 6,184,829 B1, February 6, 2001, "Calibration for Wireless Location System."

Over the past few years, the cellular industry has increased the number of air interface protocols available for use by wireless telephones, increased the number of frequency 10 bands in which wireless or mobile telephones may operate, and has expanded the number of terms that refer or relate to mobile telephones to include "personal communications services", "wireless", and others. The air interface protocols now include AMPS, N-AMPS, TDMA, CDMA, GSM, TACS, ESMR, GPRS, EDGE, and others. The changes 15 in terminology and increases in the number of air interfaces do not change the basic principles and inventions discovered and enhanced by the inventors. However, in keeping with the current terminology of the industry, the inventors now call the system described herein a *Wireless Location System*.

20 The inventors have conducted extensive experiments with the Wireless Location System technology to demonstrate both the viability and value of the technology. For example, several experiments were conducted during several months of 1995 and 1996 in the cities of Philadelphia and Baltimore to verify the system's ability to mitigate multipath in large urban environments. Then, in 1996 the inventors constructed a system in Houston that 25 was used to test the technology's effectiveness in that area and its ability to interface directly with E9-1-1 systems. Then, in 1997, the system was tested in a 350 square mile area in New Jersey and was used to locate real 9-1-1 calls from real people in trouble. Since that time, the system test has been expanded to include 125 cell sites covering an area of over 2,000 square miles. During all of these tests, techniques discussed and 30 disclosed herein were tested for effectiveness and further developed, and the system has been demonstrated to overcome the limitations of other approaches that have been proposed for locating wireless telephones.

The value and importance of the Wireless Location System has been acknowledged by the wireless communications industry. In June 1996, the Federal Communications Commission issued requirements for the wireless communications industry to deploy
5 location systems for use in locating wireless 9-1-1 callers, with a deadline of October 2001. The location of wireless E9-1-1 callers will save response time, save lives, and save enormous costs because of reduced use of emergency responses resources. In addition, numerous surveys and studies have concluded that various wireless applications, such as location sensitive billing, fleet management, and others, will have
10 great commercial values in the coming years.

Background on Wireless Communications Systems

There are many different types of air interface protocols used for wireless communications systems. These protocols are used in different frequency bands, both in
15 the U.S. and internationally. The frequency band does not impact the Wireless Location System's effectiveness at locating wireless telephones.

All air interface protocols use two types of "channels". The first type includes control channels that are used for conveying information about the wireless telephone or
20 transmitter, for initiating or terminating calls, or for transferring bursty data. For example, some types of short messaging services transfer data over the control channel. In different air interfaces, control channels are known by different terminology, but the use of the control channels in each air interface is similar. Control channels generally have identifying information about the wireless telephone or transmitter contained in the
25 transmission. Control channels also include various data transfer protocols that are not voice specific – these include General Packet Radio Service (GPRS), Enhanced Data rate for GSM Evolution (EDGE), and Enhanced GPRS (EGPRS).

The second type includes voice channels that are typically used for conveying voice
30 communications over the air interface. These channels are only used after a call has been set up using the control channels. Voice channels will typically use dedicated resources within the wireless communications system whereas control channels will use shared

resources. This distinction will generally make the use of control channels for wireless location purposes more cost effective than the use of voice channels, although there are some applications for which regular location on the voice channel is desired. Voice channels generally do not have identifying information about the wireless telephone or transmitter in the transmission. Some of the differences in the air interface protocols are discussed below:

AMPS – This is the original air interface protocol used for cellular communications in the U.S. In the AMPS system, separate dedicated channels are assigned for use by control channels (RCC). According to the TIA/EIA Standard IS-553A, every control channel block must begin at cellular channel 333 or 334, but the block may be of variable length. In the U.S., by convention, the AMPS control channel block is 21 channels wide, but the use of a 26-channel block is also known. A reverse voice channel (RVC) may occupy any channel that is not assigned to a control channel. The control channel modulation is FSK (frequency shift keying), while the voice channels are modulated using FM (frequency modulation).

N-AMPS – This air interface is an expansion of the AMPS air interface protocol, and is defined in EIA/TIA standard IS-88. The control channels are substantially the same as for AMPS; however, the voice channels are different. The voice channels occupy less than 10 KHz of bandwidth, versus the 30 KHz used for AMPS, and the modulation is FM.

TDMA – This interface is also known D-AMPS, and is defined in EIA/TIA standard IS-136. This air interface is characterized by the use of both frequency and time separation. Control channels are known as Digital Control Channels (DCCH) and are transmitted in bursts in timeslots assigned for use by DCCH. Unlike AMPS, DCCH may be assigned anywhere in the frequency band, although there are generally some frequency assignments that are more attractive than others based upon the use of probability blocks. Voice channels are known as Digital Traffic Channels (DTC). DCCH and DTC may occupy the same frequency assignments, but not the same timeslot assignment in a given

frequency assignment. DCCH and DTC use the same modulation scheme, known as $\pi/4$ DQPSK (differential quadrature phase shift keying). In the cellular band, a carrier may use both the AMPS and TDMA protocols, as long as the frequency assignments for each protocol are kept separated. A carrier may also aggregate digital channels together to support higher speed data transfer protocols such as GPRS and EDGE.

CDMA – This air interface is defined by EIA/TIA standard IS-95A. This air interface is characterized by the use of both frequency and code separation. However, because adjacent cell sites may use the same frequency sets, CDMA is also characterized by very careful power control. This careful power control leads to a situation known to those skilled in the art as the near-far problem, which makes wireless location difficult for most approaches to function properly. Control channels are known as Access Channels, and voice channels are known as Traffic Channels. Access and Traffic Channels may share the same frequency band, but are separated by code. Access and Traffic Channels use the same modulation scheme, known as OQPSK. CDMA can support higher speed data transfer protocols by aggregating codes together.

GSM - the international standard Global System for Mobile Communications defines this air interface. Like TDMA, GSM is characterized by the use of both frequency and time separation. The channel bandwidth is 200 KHz, which is wider than the 30 KHz used for TDMA. Control channels are known as Standalone Dedicated Control Channels (SDCCH), and are transmitted in bursts in timeslots assigned for use by SDCCH. SDCCH may be assigned anywhere in the frequency band. Voice channels are known as Traffic Channels (TCH). SDCCH and TCH may occupy the same frequency assignments, but not the same timeslot assignment in a given frequency assignment. SDCCH and TCH use the same modulation scheme, known as GMSK. GSM can also support higher data transfer protocols such as GPRS and EGPRS.

Within this specification the reference to any one of the air interfaces may refer to all of the air interfaces, unless specified otherwise. Additionally, a reference to control channels or voice channels may refer to all types of control or voice channels, whatever

the preferred terminology for a particular air interface. Finally, there are many more types of air interfaces used throughout the world, and there is no intent to exclude any air interface from the inventive concepts described within this specification. Indeed, those skilled in the art will recognize other interfaces used elsewhere are derivatives of or
5 similar in class to those described above.

SUMMARY OF THE INVENTION

The present invention is designed to collect wireless call associated information using a non-invasive, passive collection mechanism. The invention may be used to
10 determine cell, frequency, and caller information for purposes of directing a Wireless Location System. For example, in an overlay Wireless Location System, an Abis interface may be monitored to obtain information used to locate GSM phones. In this implementation, signaling links of the Abis interface are passively monitored to obtain certain information, such as control and traffic channel assignment, called number, and
15 mobile identification, which is not available from the GSM air interface of the reverse channel. This approach also applies to IDEN and can be broadened to include CDMA systems where the GSM architecture has been used and the system includes a separate BTS to BSC interface.

20 Other features and advantages of the invention are disclosed below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figures 1 and 1A schematically depict a Wireless Location System in accordance with the present invention.

25

Figure 2 schematically depicts a Signal Collection System (SCS) 10 in accordance with the present invention.

Figure 2A schematically depicts a receiver module 10-2 employed by the Signal
30 Collection System.

Figures 2B and 2C schematically depict alternative ways of coupling the receiver module(s) 10-2 to the antennas 10-1.

Figure 2C-1 is a flowchart of a process employed by the Wireless Location System when
5 using narrowband receiver modules.

Figure 2D schematically depicts a DSP module 10-3 employed in the Signal Collection System in accordance with the present invention.

10 Figure 2E is a flowchart of the operation of the DSP module(s) 10-3, and Figure 2E-1 is a flowchart of the process employed by the DSP modules for detecting active channels.

Figure 2F schematically depicts a Control and Communications Module 10-5 in accordance with the present invention.

15

Figures 2G-2J depict aspects of the presently preferred SCS calibration methods. Figure 2G is a schematic illustration of baselines and error values used to explain an external calibration method in accordance with the present invention. Figure 2H is a flowchart of an internal calibration method. Figure 2I is an exemplary transfer function of an AMPS
20 control channel and Figure 2J depicts an exemplary comb signal.

Figures 2K and 2L are flowcharts of two methods for monitoring performance of a Wireless Location System in accordance with the present invention.

25 Figure 3 schematically depicts a TDOA Location Processor 12 in accordance with the present invention.

Figure 3A depicts the structure of an exemplary network map maintained by the TLP controllers in accordance with the present invention.

30

Figures 4 and 4A schematically depict different aspects of an Applications Processor 14 in accordance with the present invention.

Figure 5 is a flowchart of a central station-based location processing method in accordance with the present invention.

- 5 Figure 6 is a flowchart of a station-based location processing method in accordance with the present invention.

Figure 7 is a flowchart of a method for determining, for each transmission for which a location is desired, whether to employ central or station-based processing.

10

Figure 8 is a flowchart of a dynamic process used to select cooperating antennas and SCS's 10 used in location processing.

- 15 Figure 9 is diagram that is referred to below in explaining a method for selecting a candidate list of SCS's and antennas using a predetermined set of criteria.

Figure 10 is a simplified block diagram of a monitoring system in accordance with the present invention.

- 20 Figure 11 is a flowchart of a monitoring method in accordance with the present invention.

- Figures 12A-12P schematically depict various aspects of a presently preferred implementation of the invention. Many of these depict signal formats and structures in
25 accordance with the GSM specification. In particular,

Figure 12A schematically depicts a call setup "arrow diagram" for a mobile station-originating call;

Figure 12B schematically depicts the structure of a Random Access Burst according to the GSM specification;

- 30 Figure 12C depicts the format of an RR Channel Request Message;

Figure 12D depicts the Request reference fields in the Channel Required Message;

Figure 12E depicts the Frame Number according to the GSM specification;

Figure 12F depicts Encryption Information Element within the Channel Activation Command;

Figure 12G depicts the Channel Number Information Element;

Figure 12H depicts the Channel Description Information Element;

5 Figure 12I depicts the Bit Pattern specified for CM Service Types;

Figure 12J depicts the MS Classmark Fields in a CM Service Request;

Figure 12K depicts the format of the Mobile Identity fields;

Figure 12L depicts Ciphering and Deciphering operations at the MS and BTS;

Figure 12M depicts a cascade of messages concerning Ciphering Transition among
10 the MSC, BSC, BTS and MS;

Figure 12N depicts an Encryption Information Element within the Encryption Command;

Figure 12O depicts a Called Party BCD Number; and

Figure 12P schematically depicts an exemplary system architecture for carrying out
15 the present invention.

20 DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

A goal of the present invention is to provide a mechanism for non-invasively collecting information concerning cell, frequency, and caller for purposes of directing a wireless location system. For example, the present invention provides a method that may be used in a Wireless Location System of the kind described below to locate GSM
25 mobile phones. With the architecture described below, the system would not be required to detect and demodulate messages from the mobile terminal during call setup. Instead, the WLS could ascertain call setup information from the interface between the BTS and the BSC, which is commonly called the "Abis" interface. From the Abis interface, the location system can identify the calling party (indirectly), the called party (e.g., 911), and
30 the TDMA/FDMA resource being used for a given call at any time.

The following is a description of an illustrative WLS of the kind in which the present invention may be used. This description is intended to provide the interested reader with a thorough understanding of a presently preferred environment in which the present invention may be utilized. It should be noted, however, that, except to the extent that

5 they may be expressly so limited, the claims of the present application are by no means limited to the details of the illustrative WLS described herein. Indeed, for example, the present invention is applicable to Wireless Location Systems characterized as TDOA systems, AOA systems, and hybrid TDOA/AOA systems. Following the description of the illustrative WLS, presently preferred embodiments of the inventive method for non-

10 invasively collecting call information are described.

Overview of WLS

A Wireless Location System, or WLS, may be configured to operate as a passive overlay to a wireless communications system, such as a cellular, PCS, or ESMR system,

15 although the concepts are not limited to just those types of communications systems. Wireless communications systems are generally not suitable for locating wireless devices because the designs of the wireless transmitters and cell sites do not include the necessary functionality to achieve accurate location. Accurate location in this application is defined as accuracy of 100 to 400 feet RMS (root mean square). This is distinguished

20 from the location accuracy that can be achieved by existing cell sites, which is generally limited to the radius of the cell site. In general, cell sites are not designed or programmed to cooperate between and among themselves to determine wireless transmitter location. Additionally, wireless transmitters such as cellular and PCS telephones are designed to be low cost and therefore generally do not have locating capability built-in. A WLS may

25 be designed to be a low cost addition to a wireless communications system that involves minimal changes to cell sites and no changes at all to standard wireless transmitters. The system may be considered passive because it does not contain transmitters, and therefore does not cause interference to the wireless communications system.

30 As shown in Figure 1, the Wireless Location System has four major kinds of subsystems: the Signal Collection Systems (SCS's) 10, the TDOA Location Processors (TLP's) 12, the Application Processors (AP's) 14, and the Network Operations Console (NOC) 16.

Each SCS is responsible for receiving the RF signals transmitted by the wireless transmitters on both control channels and voice channels. In general, each SCS is preferably installed at a wireless carrier's cell site, and therefore operates in parallel to a base station. Each TLP 12 is responsible for managing a network of SCS's 10 and for providing a centralized pool of digital signal processing (DSP) resources that can be used in the location calculations. The SCS's 10 and the TLP's 12 operate together to determine the location of the wireless transmitters, as will be discussed more fully below. Digital signal processing is the preferable manner in which to process radio signals because DSP's are relatively low cost, provide consistent performance, and are easily re-programmable to handle many different tasks. Both the SCS's 10 and TLP's 12 contain a significant amount of DSP resources, and the software in these systems can operate dynamically to determine where to perform a particular processing function based upon tradeoffs in processing time, communications time, queuing time, and cost. Each TLP 12 exists centrally primarily to reduce the overall cost of implementing the Wireless Location System, although the techniques discussed herein are not limited to the preferred architecture shown. That is, DSP resources can be relocated within the Wireless Location System without changing the basic concepts and functionality disclosed.

The AP's 14 are responsible for managing all of the resources in the Wireless Location System, including all of the SCS's 10 and TLP's 12. Each AP 14 also contains a specialized database that contains "triggers" for the Wireless Location System. In order to conserve resources, the Wireless Location System can be programmed to locate only certain pre-determined types of transmissions. When a transmission of a pre-determined type occurs, then the Wireless Location System is triggered to begin location processing. Otherwise, the Wireless Location System may be programmed to ignore the transmission. Each AP 14 also contains applications interfaces that permit a variety of applications to securely access the Wireless Location System. These applications may, for example, access location records in real time or non-real time, create or delete certain type of triggers, or cause the Wireless Location System to take other actions. Each AP 14 is also capable of certain post-processing functions that allow the AP 14 to combine a

number of location records to generate extended reports or analyses useful for applications such as traffic monitoring or RF optimization.

The NOC 16 is a network management system that provides operators of the Wireless Location System easy access to the programming parameters of the Wireless Location System. For example, in some cities, the Wireless Location System may contain many hundreds or even thousands of SCS's 10. The NOC is the most effective way to manage a large Wireless Location System, using graphical user interface capabilities. The NOC will also receive real time alerts if certain functions within the Wireless Location System are not operating properly. These real time alerts can be used by the operator to take corrective action quickly and prevent a degradation of location service. Experience with trials of the Wireless Location System show that the ability of the system to maintain good location accuracy over time is directly related to the operator's ability to keep the system operating within its predetermined parameters.

Readers of U.S. Patents 5,327,144 and 5,608,410 and this specification will note similarities between the respective systems. Indeed, the system disclosed herein is significantly based upon and also significantly enhanced from the system described in those previous patents. For example, the SCS 10 has been expanded and enhanced from the Antenna Site System described in U.S. Patent No. 5,608,410. The SCS 10 now has the capability to support many more antennas at a single cell site, and further can support the use of extended antennas as described below. This enables the SCS 10 to operate with the sectorized cell sites now commonly used. The SCS 10 can also transfer data from multiple antennas at a cell site to the TLP 12 instead of always combining data from multiple antennas before transfer. Additionally, the SCS 10 can support multiple air interface protocols thereby allowing the SCS 10 to function even as a wireless carrier continually changes the configuration of its system.

The TLP 12 is similar to the Central Site System disclosed in 5,608,410, but has also been expanded and enhanced. For example, the TLP 12 has been made scaleable so that the amount of DSP resources required by each TLP 12 can be appropriately scaled to match the number of locations per second required by customers of the Wireless

Location System. In order to support scaling for different Wireless Location System capacities, a networking scheme has been added to the TLP 12 so that multiple TLP's 12 can cooperate to share RF data across wireless communication system network boundaries. Additionally, the TLP 12 has been given control means to determine the SCS's 10, and more importantly the antennas at each of the SCS's 10, from which the TLP 12 is to receive data in order to process a specific location. Previously, the Antenna Site Systems automatically forwarded data to the Central Site System, whether requested or not by the Central Site System. Furthermore, the SCS 10 and TLP 12 combined have been designed with additional means for removing multipath from the received transmissions.

The Database Subsystem of the Central Site System has been expanded and developed into the AP 14. The AP 14 can support a greater variety of applications than previously disclosed in 5,608,410, including the ability to post-process large volumes of location records from multiple wireless transmitters. This post-processed data can yield, for example, very effective maps for use by wireless carriers to improve and optimize the RF design of the communications systems. This can be achieved, for example, by plotting the locations of all of the callers in an area and the received signal strengths at a number of cell sites. The carrier can then determine whether each cell site is, in fact, serving the exact coverage area desired by the carrier. The AP 14 can also now store location records anonymously, that is, with the MIN and/or other identity information removed from the location record, so that the location record can be used for RF optimization or traffic monitoring without causing concerns about an individual user's privacy.

As shown in Figure 1A, a presently preferred implementation of the Wireless Location System includes a plurality of SCS regions each of which comprises multiple SCS's 10. For example, "SCS Region 1" includes SCS's 10A and 10B (and preferably others, not shown) that are located at respective cell sites and share antennas with the base stations at those cell sites. Drop and insert units 11A and 11B are used to interface fractional T1/E1 lines to full T1/E1 lines, which in turn are coupled to a digital access and control system (DACS) 13A. The DACS 13A and another DACS 13B are used in the manner described more fully below for communications between the SCS's 10A, 10B, etc., and

multiple TLP's 12A, 12B, etc. As shown, the TLP's are typically collocated and interconnected via an Ethernet network (backbone) and a second, redundant Ethernet network. Also coupled to the Ethernet networks are multiple AP's 14A and 14B, multiple NOC's 16A and 16B, and a terminal server 15. Routers 19A and 19B are used to couple
5 one Wireless Location System to one or more other Wireless Location System(s).

Signal Collection System 10

Generally, cell sites will have one of the following antenna configurations: (i) an omnidirectional site with 1 or 2 receive antennas or (ii) a sectored site with 1, 2, or 3
10 sectors, and with 1 or 2 receive antennas used in each sector. As the number of cell sites has increased in the U.S. and internationally, sectored cell sites have become the predominant configuration. However, there are also a growing number of micro-cells and pico-cells, which can be omnidirectional. Therefore, the SCS 10 has been designed to be configurable for any of these typical cell sites and has been provided with mechanisms to
15 employ any number of antennas at a cell site.

The basic architectural elements of the SCS 10 remain the same as for the Antenna Site System described in 5,608,410, but several enhancements have been made to increase the flexibility of the SCS 10 and to reduce the commercial deployment cost of the system.
20 The most presently preferred embodiment of the SCS 10 is described herein. The SCS 10, an overview of which is shown in Figure 2, includes digital receiver modules 10-2A through 10-2C; DSP modules 10-3A through 10-3C; a serial bus 10-4, a control and communications module 10-5; a GPS module 10-6; and a clock distribution module 10-7. The SCS 10 has the following external connections: power, fractional T1/E1
25 communications, RF connections to antennas, and a GPS antenna connection for the timing generation (or clock distribution) module 10-7. The architecture and packaging of the SCS 10 permit it to be physically collocated with cell sites (which is the most common installation place), located at other types of towers (such as FM, AM, two-way emergency communications, television, etc.), or located at other building structures (such
30 as rooftops, silos, etc.).

Timing Generation

The Wireless Location System depends upon the accurate determination of time at all SCS's 10 contained within a network. Several different timing generation systems have been described in previous disclosures, however the most presently preferred embodiment is based upon an enhanced GPS receiver 10-6. The enhanced GPS receiver differs from most traditional GPS receivers in that the receiver contains algorithms that remove some of the timing instability of the GPS signals, and guarantees that any two SCS's 10 contained within a network can receive timing pulses that are within approximately ten nanoseconds of each other. These enhanced GPS receivers are now commercially available, and further reduce some of the time reference related errors that were observed in previous implementations of wireless location systems. While this enhanced GPS receiver can produce a very accurate time reference, the output of the receiver may still have an unacceptable phase noise. Therefore, the output of the receiver is input to a low phase noise, crystal oscillator-driven phase locked loop circuit that can now produce 10 MHz and one pulse per second (PPS) reference signals with less than 0.01 degrees RMS of phase noise, and with the pulse output at any SCS 10 in a Wireless Location System network within ten nanoseconds of any other pulse at another SCS 10. This combination of enhanced GPS receiver, crystal oscillator, and phase locked loop is now the most preferred method to produce stable time and frequency reference signals with low phase noise.

The SCS 10 has been designed to support multiple frequency bands and multiple carriers with equipment located at the same cell site. This can take place by using multiple receivers internal to a single SCS chassis, or by using multiple chassis each with separate receivers. In the event that multiple SCS chassis are placed at the same cell site, the SCS's 10 can share a single timing generation/clock distribution circuit 10-7 and thereby reduce overall system cost. The 10 MHz and one PPS output signals from the timing generation circuit are amplified and buffered internal to the SCS 10, and then made available via external connectors. Therefore a second SCS can receive its timing from a first SCS using the buffered output and the external connectors. These signals can also be made available to base station equipment collocated at the cell site. This might be useful

to the base station, for example, in improving the frequency re-use pattern of a wireless communications system.

Receiver Module 10-2 (Wideband Embodiment)

5 When a wireless transmitter makes a transmission, the Wireless Location System must receive the transmission at multiple SCS's 10 located at multiple geographically dispersed cell sites. Therefore, each SCS 10 has the ability to receive a transmission on any RF channel on which the transmission may originate. Additionally, since the SCS 10 is capable of supporting multiple air interface protocols, the SCS 10 also supports
10 multiple types of RF channels. This is in contrast to most current base station receivers, which typically receive only one type of channel and are usually capable of receiving only on select RF channels at each cell site. For example, a typical TDMA base station receiver will only support 30 KHz wide channels, and each receiver is programmed to receive signals on only a single channel whose frequency does not change often (i.e.
15 there is a relatively fixed frequency plan). Therefore, very few TDMA base station receivers would receive a transmission on any given frequency. As another example, even though some GSM base station receivers are capable of frequency hopping, the receivers at multiple base stations are generally not capable of simultaneously tuning to a single frequency for the purpose of performing location processing. In fact, the receivers
20 at GSM base stations are programmed to frequency hop to avoid using an RF channel that is being used by another transmitter so as to minimize interference.

The SCS receiver module 10-2 is preferably a dual wideband digital receiver that can receive the entire frequency band and all of the RF channels of an air interface. For
25 cellular systems in the U.S., this receiver module is either 15 MHz wide or 25 MHz wide so that all of the channels of a single carrier or all of the channels of both carriers can be received. This receiver module has many of the characteristics of the receiver previously described in Patent Number 5,608,410, and Figure 2A is a block diagram of the currently preferred embodiment. Each receiver module contains an RF tuner section 10-2-1, a data
30 interface and control section 10-2-2 and an analog to digital conversion section 10-2-3. The RF tuner section 10-2-1 includes two full independent digital receivers (including Tuner #1 and Tuner #2) that convert the analog RF input from an external connector into

a digitized data stream. Unlike most base station receivers, the SCS receiver module does not perform diversity combining or switching. Rather, the digitized signal from each independent receiver is made available to the location processing. The present inventors have determined that there is an advantage to the location processing, and especially the multipath mitigation processing, to independently process the signals from each antenna rather than perform combining on the receiver module.

The receiver module 10-2 performs, or is coupled to elements that perform, the following functions: automatic gain control (to support both nearby strong signals and far away weak signals), bandpass filtering to remove potentially interfering signals from outside of the RF band of interest, synthesis of frequencies needed for mixing with the RF signals to create an IF signal that can be sampled, mixing, and analog to digital conversion (ADC) for sampling the RF signals and outputting a digitized data stream having an appropriate bandwidth and bit resolution. The frequency synthesizer locks the synthesized frequencies to the 10 MHz reference signal from the clock distribution/timing generation module 10-7 (Figure 2). All of the circuits used in the receiver module maintain the low phase noise characteristics of the timing reference signal. The receiver module preferably has a spurious free dynamic range of at least 80 dB.

The receiver module 10-2 also contains circuits to generate test frequencies and calibration signals, as well as test ports where measurements can be made by technicians during installation or troubleshooting. Various calibration processes are described in further detail below. The internally generated test frequencies and test ports provide an easy method for engineers and technicians to rapidly test the receiver module and diagnose any suspected problems. This is also especially useful during the manufacturing process.

One of the advantages of the Wireless Location System described herein is that no new antennas are required at cell sites. The Wireless Location System can use the existing antennas already installed at most cell sites, including both omni-directional and sectorized antennas. This feature can result in significant savings in the installation and

maintenance costs of the Wireless Location System versus other approaches that have been described in the prior art. The SCS's digital receivers 10-2 can be connected to the existing antennas in two ways, as shown in Figures 2B and 2C, respectively. In Figure 2B, the SCS receivers 10-2 are connected to the existing cell site multi-coupler or RF splitter. In this manner, the SCS 10 uses the cell site's existing low noise pre-amplifier, band pass filter, and multi-coupler or RF splitter. This type of connection usually limits the SCS 10 to supporting the frequency band of a single carrier. For example, an A-side cellular carrier will typically use the band pass filter to block signals from customers of the B-side carrier, and vice versa.

10

In Figure 2C, the existing RF path at the cell site has been interrupted, and a new pre-amplifier, band pass filter, and RF splitter has been added as part of the Wireless Location System. The new band pass filter will pass multiple contiguous frequency bands, such as both the A-side and B-side cellular carriers, thereby allowing the Wireless Location System to locate wireless transmitters using both cellular systems but using the antennas from a single cell site. In this configuration, the Wireless Location System uses matched RF components at each cell site, so that the phase versus frequency responses are identical. This is in contrast to existing RF components, which may be from different manufacturers or using different model numbers at various cell sites. Matching the response characteristics of RF components reduces a possible source of error for the location processing, although the Wireless Location System has the capability to compensate for these sources of error. Finally, the new pre-amplifier installed with the Wireless Location System will have a very low noise figure to improve the sensitivity of the SCS 10 at a cell site. The overall noise figure of the SCS digital receivers 10-2 is dominated by the noise figure of the low noise amplifiers. Because the Wireless Location System can use weak signals in location processing, whereas the base station typically cannot process weak signals, the Wireless Location System can significantly benefit from a high quality, very low noise amplifier.

20

25

30

In order to improve the ability of the Wireless Location System to accurately determine TDOA for a wireless transmission, the phase versus frequency response of the cell site's RF components are determined at the time of installation and updated at other certain

times and then stored in a table in the Wireless Location System. This can be important because, for example, the band pass filters and/or multi-couplers made by some manufacturers have a steep and non-linear phase versus frequency response near the edge of the pass band. If the edge of the pass band is very near to or coincident with the reverse control or voice channels, then the Wireless Location System would make incorrect measurements of the transmitted signal's phase characteristics if the Wireless Location System did not correct the measurements using the stored characteristics. This becomes even more important if a carrier has installed multi-couplers and/or band pass filters from more than one manufacturer, because the characteristics at each site may be different. In addition to measuring the phase versus frequency response, other environmental factors may cause changes to the RF path prior to the ADC. These factors require occasional and sometimes periodic calibration in the SCS 10.

Alternative Narrowband Embodiment of Receiver Module 10-2

In addition or as an alternative to the wideband receiver module, the SCS 10 also supports a narrowband embodiment of the receiver module 10-2. In contrast to the wideband receiver module that can simultaneously receive all of the RF channels in use by a wireless communications system, the narrowband receiver can only receive one or a few RF channels at a time. For example, the SCS 10 supports a 60 KHz narrowband receiver for use in AMPS/TDMA systems, covering two contiguous 30 KHz channels. This receiver is still a digital receiver as described for the wideband module, however the frequency synthesizing and mixing circuits are used to dynamically tune the receiver module to various RF channels on command. This dynamic tuning can typically occur in one millisecond or less, and the receiver can dwell on a specific RF channel for as long as required to receive and digitize RF data for location processing.

The purpose of the narrowband receiver is to reduce the implementation cost of a Wireless Location System from the cost that is incurred with wideband receivers. Of course, there is some loss of performance, but the availability of these multiple receivers permits wireless carriers to have more cost/performance options. Additional inventive functions and enhancements have been added to the Wireless Location System to support this new type of narrowband receiver. When the wideband receiver is being used, all RF

channels are received continuously at all SCS's 10, and subsequent to the transmission, the Wireless Location System can use the DSP's 10-3 (Figure 2) to dynamically select any RF channel from the digital memory. With the narrowband receiver, the Wireless Location System must ensure *a priori* that the narrowband receivers at multiple cell sites
5 are simultaneously tuned to the same RF channel so that all receivers can simultaneously receive, digitize and store the same wireless transmission. For this reason, the narrowband receiver is generally used only for locating voice channel transmissions, which can be known *a priori* to be making a transmission. Since control channel transmissions can occur asynchronously at any time, the narrowband receiver may not be
10 tuned to the correct channel to receive the transmission.

When the narrowband receivers are used for locating AMPS voice channel transmissions, the Wireless Location System has the ability to temporarily change the modulation characteristics of the AMPS wireless transmitter to aid location processing.
15 This may be necessary because AMPS voice channels are only FM modulated with the addition of a low level supervisory tone known as SAT. As is known in the art, the Cramer-Rao lower bound of AMPS FM modulation is significantly worse than the Manchester encoded FSK modulation used for AMPS reverse channels and "blank and burst" transmissions on the voice channel. Further, AMPS wireless transmitters may be
20 transmitting with significantly reduced energy if there is no modulating input signal (i.e., no one is speaking). To improve the location estimate by improving the modulation characteristics without depending on the existence or amplitude of an input modulating signal, the Wireless Location System can cause an AMPS wireless transmitter to transmit a "blank and burst" message at a point in time when the narrowband receivers at multiple
25 SCS's 10 are tuned to the RF channel on which the message will be sent. This is further described later.

The Wireless Location System performs the following steps when using the narrowband receiver module (see the flowchart of Figure 2C-1):

- 30 a first wireless transmitter is *a priori* engaged in transmitting on a particular RF channel;

the Wireless Location System triggers to make a location estimate of the first wireless transmitter (the trigger may occur either internally or externally via a command/response interface);

the Wireless Location System determines the cell site, sector, RF channel, timeslot,
5 long code mask, and encryption key (all information elements may not be necessary for all air interface protocols) currently in use by the first wireless transmitter;

the Wireless Location System tunes an appropriate first narrowband receiver at an appropriate first SCS 10 to the RF channel and timeslot at the designated cell site and sector, wherein appropriate typically means both available and collocated or
10 in closest proximity;

the first SCS 10 receives a time segment of RF data, typically ranging from a few microseconds to tens of milliseconds, from the first narrowband receiver and evaluates the transmission's power, SNR, and modulation characteristics;

15 if the transmission's power or SNR is below a predetermined threshold, the Wireless Location System waits a predetermined length of time and then returns to the above third step (where the Wireless Location System determines the cell site, sector, etc.);

if the transmission is an AMPS voice channel transmission and the modulation is
20 below a threshold, then the Wireless Location System commands the wireless communications system to send a command to the first wireless transmitter to cause a "blank and burst" on the first wireless transmitter;

the Wireless Location System requests the wireless communications system to prevent hand-off of the wireless transmitter to another RF channel for a
25 predetermined length of time;

the Wireless Location System receives a response from the wireless communications system indicating the time period during which the first wireless transmitter will be prevented from handing-off, and if commanded, the time period during which the wireless communications system will send a command to the first wireless
30 transmitter to cause a "blank and burst";

the Wireless Location System determines the list of antennas that will be used in location processing (the antenna selection process is described below);

the Wireless Location System determines the earliest Wireless Location System timestamp at which the narrowband receivers connected to the selected antennas are available to begin simultaneously collecting RF data from the RF channel currently in use by the first wireless transmitter;

5 based upon the earliest Wireless Location System timestamp and the time periods in the response from the wireless communications system, the Wireless Location System commands the narrowband receivers connected to the antennas that will be used in location processing to tune to the cell site, sector, and RF channel currently in use by the first wireless transmitter and to receive RF data for a

10 predetermined dwell time (based upon the bandwidth of the signal, SNR, and integration requirements);

the RF data received by the narrowband receivers are written into the dual port memory;

location processing on the received RF data commences, as described in Patent Nos.

15 5,327,144 and 5,608,410 and in sections below;

the Wireless Location System again determines the cell site, sector, RF channel, timeslot, long code mask, and encryption key currently in use by the first wireless transmitter;

if the cell site, sector, RF channel, timeslot, long code mask, and encryption key

20 currently in use by the first wireless transmitter has changed between queries (i.e. before and after gathering the RF data) the Wireless Location System ceases location processing, causes an alert message that location processing failed because the wireless transmitter changed transmission status during the period of time in which RF data was being received, and re-triggers this entire process;

25 location processing on the received RF data completes in accordance with the steps described below.

The determination of the information elements including cell site, sector, RF channel, timeslot, long code mask, and encryption key (all information elements may not be

30 necessary for all air interface protocols) is typically obtained by the Wireless Location System through a command / response interface between the Wireless Location System and the wireless communications system.

The use of the narrowband receiver in the manner described above is known as random tuning because the receivers can be directed to any RF channel on command from the system. One advantage to random tuning is that locations are processed only for those
5 wireless transmitters for which the Wireless Location System is triggered. One disadvantage to random tuning is that various synchronization factors, including the interface between the wireless communications system and the Wireless Location System and the latency times in scheduling the necessary receivers throughout the system, can limit the total location processing throughput. For example, in a TDMA
10 system, random tuning used throughout the Wireless Location System will typically limit location processing throughput to about 2.5 locations per second per cell site sector.

Therefore, the narrowband receiver also supports another mode, known as automatic sequential tuning, which can perform location processing at a higher throughput. For
15 example, in a TDMA system, using similar assumptions about dwell time and setup time as for the narrowband receiver operation described above, sequential tuning can achieve a location processing throughput of about 41 locations per second per cell site sector, meaning that all 395 TDMA RF channels can be processed in about 9 seconds. This increased rate can be achieved by taking advantage of, for example, the two contiguous
20 RF channels that can be received simultaneously, location processing all three TDMA timeslots in an RF channel, and eliminating the need for synchronization with the wireless communications system. When the Wireless Location System is using the narrowband receivers for sequential tuning, the Wireless Location System has no knowledge of the identity of the wireless transmitter because the Wireless Location
25 System does not wait for a trigger, nor does the Wireless Location System query the wireless communications system for the identity information prior to receiving the transmission. In this method, the Wireless Location System sequences through every cell site, RF channel and time slot, performs location processing, and reports a location record identifying a time stamp, cell site, RF channel, time slot, and location. Subsequent
30 to the location record report, the Wireless Location System and the wireless communications system match the location records to the wireless communications system's data indicating which wireless transmitters were in use at the time, and which

cell sites, RF channels, and time slots were used by each wireless transmitter. Then, the Wireless Location System can retain the location records for wireless transmitters of interest, and discard those location records for the remaining wireless transmitters.

5 Digital Signal Processor Module 10-3

The SCS digital receiver modules 10-2 output a digitized RF data stream having a specified bandwidth and bit resolution. For example, a 15 MHz embodiment of the wideband receiver may output a data stream containing 60 million samples per second, at a resolution of 14 bits per sample. This RF data stream will contain all of the RF
10 channels that are used by the wireless communications system. The DSP modules 10-3 receive the digitized data stream, and can extract any individual RF channel through digital mixing and filtering. The DSP's can also reduce the bit resolution upon command from the Wireless Location System, as needed to reduce the bandwidth requirements between the SCS 10 and TLP 12. The Wireless Location System can dynamically select
15 the bit resolution at which to forward digitized baseband RF data, based upon the processing requirements for each location. DSP's are used for these functions to reduce the systemic errors that can occur from mixing and filtering with analog components. The use of DSP's allows perfect matching in the processing between any two SCS's 10.

20 A block diagram of the DSP module 10-3 is shown in Figure 2D, and the operation of the DSP module is depicted by the flowchart of Figure 2E. As shown in Figure 2D, the DSP module 10-3 comprises the following elements: a pair of DSP elements 10-3-1A and 10-3-1B, referred to collectively as a "first" DSP; serial to parallel converters 10-3-2; dual port memory elements 10-3-3; a second DSP 10-3-4; a parallel to serial converter; a
25 FIFO buffer; a DSP 10-3-5 (including RAM) for detection, another DSP 10-3-6 for demodulation, and another DSP 10-3-7 for normalization and control; and an address generator 10-3-8. In a presently preferred embodiment, the DSP module 10-3 receives the wideband digitized data stream (Figure 2E, step S1), and uses the first DSP (10-3-1A and 10-3-1B) to extract blocks of channels (step S2). For example, a first DSP
30 programmed to operate as a digital drop receiver can extract four blocks of channels, wherein each block includes at least 1.25 MHz of bandwidth. This bandwidth can include 42 channels of AMPS or TDMA, 6 channels of GSM, or 1 channel of CDMA.

The DSP does not require the blocks to be contiguous, as the DSP can independently digitally tune to any set of RF channels within the bandwidth of the wideband digitized data stream. The DSP can also perform wideband or narrow band energy detection on all or any of the channels in the block, and report the power levels by channel to the TLP 12 (step S3). For example, every 10 ms, the DSP can perform wideband energy detection and create an RF spectral map for all channels for all receivers (see step S9). Because this spectral map can be sent from the SCS 10 to the TLP 12 every 10 ms via the communications link connecting the SCS 10 and the TLP 12, a significant data overhead could exist. Therefore, the DSP reduces the data overhead by companding the data into a finite number of levels. Normally, for example, 84 dB of dynamic range could require 14 bits. In the companding process implemented by the DSP, the data is reduced, for example, to only 4 bits by selecting 16 important RF spectral levels to send to the TLP 12. The choice of the number of levels, and therefore the number of bits, as well as the representation of the levels, can be automatically adjusted by the Wireless Location System. These adjustments are performed to maximize the information value of the RF spectral messages sent to the TLP 12 as well as to optimize the use of the bandwidth available on the communications link between the SCS 10 and the TLP 12.

After conversion, each block of RF channels (each at least 1.25 MHz) is passed through serial to parallel converter 10-3-2 and then stored in dual port digital memory 10-3-3 (step S4). The digital memory is a circular memory, which means that the DSP module begins writing data into the first memory address and then continues sequentially until the last memory address is reached. When the last memory address is reached, the DSP returns to the first memory address and continues to sequentially write data into memory. Each DSP module typically contains enough memory to store several seconds of data for each block of RF channels to support the latency and queuing times in the location process.

In the DSP module, the memory address at which digitized and converted RF data is written into memory is the time stamp used throughout the Wireless Location System and which the location processing references in determining TDOA. In order to ensure that the time stamps are aligned at every SCS 10 in the Wireless Location System, the

address generator 10-3-8 receives the one pulse per second signal from the timing generation/clock distribution module 10-7 (Figure 2). Periodically, the address generator at all SCS's 10 in a Wireless Location System will simultaneously reset themselves to a known address. This enables the location processing to reduce or eliminate accumulated
5 timing errors in the recording of time stamps for each digitized data element.

The address generator 10-3-8 controls both writing to and reading from the dual port digital memory 10-3-3. Writing takes places continuously since the ADC is continuously sampling and digitizing RF signals and the first DSP (10-3-1A and 10-3-1B) is
10 continuously performing the digital drop receiver function. However, reading occurs in bursts as the Wireless Location System requests data for performing demodulation and location processing. The Wireless Location System may even perform location processing recursively on a single transmission, and therefore requires access to the same data multiple times. In order to service the many requirements of the Wireless Location
15 System, the address generator allows the dual port digital memory to be read at a rate faster than the writing occurs. Typically, reading can be performed eight times faster than writing.

The DSP module 10-3 uses the second DSP 10-3-4 to read the data from the digital
20 memory 10-3-3, and then performs a second digital drop receiver function to extract baseband data from the blocks of RF channels (step S5). For example, the second DSP can extract any single 30 KHz AMPS or TDMA channel from any block of RF channels that have been digitized and stored in the memory. Likewise, the second DSP can extract any single GSM channel. The second DSP is not required to extract a CDMA channel,
25 since the channel bandwidth occupies the full bandwidth of the stored RF data. The combination of the first DSP 10-3-1A, 10-3-1B and the second DSP 10-3-4 allows the DSP module to select, store, and recover any single RF channel in a wireless communications system. A DSP module typically will store four blocks of channels. In a dual-mode AMPS/TDMA system, a single DSP module can continuously and
30 simultaneously monitor up to 42 analog reverse control channels, up to 84 digital control channels, and also be tasked to monitor and locate any voice channel transmission. A single SCS chassis will typically support up to three receiver modules 10-2 (Figure 2), to

cover three sectors of two antennas each, and up to nine DSP modules (three DSP modules per receiver permits an entire 15 MHz bandwidth to be simultaneously stored into digital memory). Thus, the SCS 10 is a very modular system than can be easily scaled to match any type of cell site configuration and processing load.

5

The DSP module 10-3 also performs other functions, including automatic detection of active channels used in each sector (step S6), demodulation (step S7), and station based location processing (step S8). The Wireless Location System maintains an active map of the usage of the RF channels in a wireless communications system (step S9), which
10 enables the Wireless Location System to manage receiver and processing resources, and to rapidly initiate processing when a particular transmission of interest has occurred. The active map comprises a table maintained within the Wireless Location System that lists for each antenna connected to an SCS 10 the primary channels assigned to that SCS 10 and the protocols used in those channels. A primary channel is an RF control channel
15 assigned to a collocated or nearby base station which the base station uses for communications with wireless transmitters. For example, in a typical cellular system with sectorized cell sites, there will be one RF control channel frequency assigned for use in each sector. Those control channel frequencies would typically be assigned as primary channels for a collocated SCS 10.

20

The same SCS 10 may also be assigned to monitor the RF control channels of other nearby base stations as primary channels, even if other SCS's 10 also have the same primary channels assigned. In this manner, the Wireless Location System implements a system demodulation redundancy that ensures that any given wireless transmission has
25 an infinitesimal probability of being missed. When this demodulation redundancy feature is used, the Wireless Location System will receive, detect, and demodulate the same wireless transmission two or more times at more than one SCS 10. The Wireless Location System includes means to detect when this multiple demodulation has occurred and to trigger location processing only once. This function conserves the processing and
30 communications resources of the Wireless Location System, and is further described below. This ability for a single SCS 10 to detect and demodulate wireless transmissions occurring at cell sites not collocated with the SCS 10 permits operators of the Wireless

Location System to deploy more efficient Wireless Location System networks. For example, the Wireless Location System may be designed such that the Wireless Location System uses much fewer SCS's 10 than the wireless communications system has base stations.

5

In the Wireless Location System, primary channels are entered and maintained in the table using two methods: direct programming and automatic detection. Direct programming comprises entering primary channel data into the table using one of the Wireless Location System user interfaces, such as the Network Operations Console 16 (Figure 1), or by receiving channel assignment data from the Wireless Location System to wireless communications system interface. Alternatively, the DSP module 10-3 also runs a background process known as automatic detection in which the DSP uses spare or scheduled processing capacity to detect transmissions on various possible RF channels and then attempt to demodulate those transmissions using probable protocols. The DSP module can then confirm that the primary channels directly programmed are correct, and can also quickly detect changes made to channels at base station and send an alert to the operator of the Wireless Location System.

The DSP module performs the following steps in automatic detection (see Figure 2E-1):

- 20 for each possible control and/or voice channel which may be used in the coverage area of the SCS 10, peg counters are established (step S7-1);
- at the start of a detection period, all peg counters are reset to zero (step S7-2);
- each time that a transmission occurs in a specified RF channel, and the received power level is above a particular pre-set threshold, the peg counter for that channel
- 25 is incremented (step S7-3);
- each time that a transmission occurs in a specified RF channel, and the received power level is above a second particular pre-set threshold, the DSP module attempts to demodulate a certain portion of the transmission using a first preferred protocol (step S7-4);
- 30 if the demodulation is successful, a second peg counter for that channel is incremented (step S7-5);

- if the demodulation is unsuccessful, the DSP module attempts to demodulate a portion of the transmission using a second preferred protocol (step S7-6);
if the demodulation is successful, a third peg counter for that channel is incremented (step S7-7);
- 5 at the end of a detection period, the Wireless Location System reads all peg counters (step S7-8); and
the Wireless Location System automatically assigns primary channels based upon the peg counters (step S7-9).
- 10 The operator of the Wireless Location System can review the peg counters and the automatic assignment of primary channels and demodulation protocols, and override any settings that were performed automatically. In addition, if more than two preferred protocols may be used by the wireless carrier, then the DSP module 10-3 can be downloaded with software to detect the additional protocols. The architecture of the SCS
- 15 10, based upon wideband receivers 10-2, DSP modules 10-3, and downloadable software permits the Wireless Location System to support multiple demodulation protocols in a single system. There is a significant cost advantage to supporting multiple protocols within the single system, as only a single SCS 10 is required at a cell site. This is in contrast to many base station architectures, which may require different transceiver
- 20 modules for different modulation protocols. For example, while the SCS 10 could support AMPS, TDMA, and CDMA simultaneously in the same SCS 10, there is no base station currently available that can support this functionality.

The ability to detect and demodulate multiple protocols also includes the ability to

25 independently detect the use of authentication in messages transmitted over the certain air interface protocols. The use of authentication fields in wireless transmitters started to become prevalent within the last few years as a means to reduce the occurrence of fraud in wireless communications systems. However, not all wireless transmitters have implemented authentication. When authentication is used, the protocol generally inserts

30 an additional field into the transmitted message. Frequently this field is inserted between the identity of the wireless transmitter and the dialed digits in the transmitted message. When demodulating a wireless transmission, the Wireless Location System determines

the number of fields in the transmitted message, as well as the message type (i.e. registration, origination, page response, etc.). The Wireless Location System demodulates all fields and if extra fields appear to be present, giving consideration to the type of message transmitted, then the Wireless Location System tests all fields for a trigger condition. For example, if the dialed digits "911" appear in the proper place in a field, and the field is located either in its proper place without authentication or its proper place with authentication, then the Wireless Location System triggers normally. In this example, the digits "911" would be required to appear in sequence as "911" or "*911", with no other digits before or after either sequence. This functionality reduces or eliminates a false trigger caused by the digits "911" appearing as part of an authentication field.

The support for multiple demodulation protocols is important for the Wireless Location System to successfully operate because location processing must be quickly triggered when a wireless caller has dialed "911". The Wireless Location System can trigger location processing using two methods: the Wireless Location System will independently demodulate control channel transmissions, and trigger location processing using any number of criteria such as dialed digits, or the Wireless Location System may receive triggers from an external source such as the carrier's wireless communications system. The present inventors have found that independent demodulation by the SCS 10 results in the fastest time to trigger, as measured from the moment that a wireless user presses the "SEND" or "TALK" (or similar) button on a wireless transmitter.

Control and Communications Module 10-5

The control and communications module 10-5, depicted in Figure 2F, includes data buffers 10-5-1, a controller 10-5-2, memory 10-5-3, a CPU 10-5-4 and a T1/E1 communications chip 10-5-5. The module has many of the characteristics previously described in Patent Number 5,608,410. Several enhancements have been added in the present embodiment. For example, the SCS 10 now includes an automatic remote reset capability, even if the CPU on the control and communications module ceases to execute its programmed software. This capability can reduce the operating costs of the Wireless Location System because technicians are not required to travel to a cell site to reset an

SCS 10 if it fails to operate normally. The automatic remote reset circuit operates by monitoring the communications interface between the SCS 10 and the TLP 12 for a particular sequence of bits. This sequence of bits is a sequence that does not occur during normal communications between the SCS 10 and the TLP 12. This sequence, for
5 example, may consist of an all ones pattern. The reset circuit operates independently of the CPU so that even if the CPU has placed itself in a locked or other non-operating status, the circuit can still achieve the reset of the SCS 10 and return the CPU to an operating status.

10 This module now also has the ability to record and report a wide variety of statistics and variables used in monitoring or diagnosing the performance of the SCS 10. For example, the SCS 10 can monitor the percent capacity usage of any DSP or other processor in the SCS 10, as well as the communications interface between the SCS 10 and the TLP 12. These values are reported regularly to the AP 14 and the NOC 16, and are used to
15 determine when additional processing and communications resources are required in the system. For example, alarm thresholds may be set in the NOC to indicate to an operator if any resource is consistently exceeding a preset threshold. The SCS 10 can also monitor the number of times that transmissions have been successfully demodulated, as well as the number of failures. This is useful in allowing operators to determine whether the
20 signal thresholds for demodulation have been set optimally.

This module, as well as the other modules, can also self-report its identity to the TLP 12. As described below, many SCS's 10 can be connected to a single TLP 12. Typically, the communications between SCS's 10 and TLP's 12 is shared with the communications
25 between base stations and MSC's. It is frequently difficult to quickly determine exactly which SCS's 10 have been assigned to particular circuits. Therefore, the SCS 10 contains a hard coded identity, which is recorded at the time of installation. This identity can be read and verified by the TLP 12 to positively determine which SCS 10 has been assigned by a carrier to each of several different communications circuits.

30

The SCS to TLP communications supports a variety of messages, including: commands and responses, software download, status and heartbeat, parameter download, diagnostic,

spectral data, phase data, primary channel demodulation, and RF data. The communications protocol is designed to optimize Wireless Location System operation by minimizing the protocol overhead and the protocol includes a message priority scheme. Each message type is assigned a priority, and the SCS 10 and the TLP 12 will queue
5 messages by priority such that a higher priority message is sent before a lower priority message is sent. For example, demodulation messages are generally set at a high priority because the Wireless Location System must trigger location processing on certain types of calls (i.e., E9-1-1) without delay. Although higher priority messages are queued before lower priority messages, the protocol generally does not preempt a message that is
10 already in transit. That is, a message in the process of being sent across the SCS 10 to TLP 12 communications interface will be completed fully, but then the next message to be sent will be the highest priority message with the earliest time stamp. In order to minimize the latency of high priority messages, long messages, such as RF data, are sent in segments. For example, the RF data for a full 100-millisecond AMPS transmission
15 may be separated into 10-millisecond segments. In this manner, a high priority message may be queued in between segments of the RF data.

Calibration and Performance Monitoring

The architecture of the SCS 10 is heavily based upon digital technologies
20 including the digital receiver and the digital signal processors. Once RF signals have been digitized, timing, frequency, and phase differences can be carefully controlled in the various processes. More importantly, any timing, frequency, and phase differences can be perfectly matched between the various receivers and various SCS's 10 used in the Wireless Location System. However, prior to the ADC, the RF signals pass through a
25 number of RF components, including antennas, cables, low noise amplifiers, filters, duplexors, multi-couplers, and RF splitters. Each of these RF components has characteristics important to the Wireless Location System, including delay and phase versus frequency response. When the RF and analog components are perfectly matched between the pairs of SCS's 10, such as SCS 10A and SCS 10B in Figure 2G, then the
30 effects of these characteristics are automatically eliminated in the location processing. But when the characteristics of the components are not matched, then the location processing can inadvertently include instrumental errors resulting from the mismatch.

Additionally, many of these RF components can experience instability with power, time, temperature, or other factors that can add instrumental errors to the determination of location. Therefore, several inventive techniques have been developed to calibrate the RF components in the Wireless Location System and to monitor the performance of the
5 Wireless Location System on a regular basis. Subsequent to calibration, the Wireless Location System stores the values of these delays and phases versus frequency response (i.e. by RF channel number) in a table in the Wireless Location System for use in correcting these instrumental errors. Figures 2G-2J are referred to below in explaining these calibration methods.

10

External Calibration Method

Referring to Figure 2G, the timing stability of the Wireless Location System is measured along baselines, wherein each baseline is comprised of two SCS's, 10A and 10B, and an imaginary line (A - B) drawn between them. In a TDOA / FDOA type of
15 Wireless Location System, locations of wireless transmitters are calculated by measuring the differences in the times that each SCS 10 records for the arrival of the signal from a wireless transmitter. Thus, it is important that the differences in times measured by SCS's 10 along any baseline are largely attributed to the transmission time of the signal from the wireless transmitter and minimally attributed to the variations in the RF and
20 analog components of the SCS's 10 themselves. To meet the accuracy goals of the Wireless Location System, the timing stability for any pair of SCS's 10 are maintained at much less than 100 nanoseconds RMS (root mean square). Thus, the components of the Wireless Location System will contribute less than 100 feet RMS of instrumentation error in the estimation of the location of a wireless transmitter. Some of this error is
25 allocated to the ambiguity of the signal used to calibrate the system. This ambiguity can be determined from the well-known Cramer-Rao lower bound equation. In the case of an AMPS reverse control channel, this error is approximately 40 nanoseconds RMS. The remainder of the error budget is allocated to the components of the Wireless Location System, primarily the RF and analog components in the SCS 10.

30

In the external calibration method, the Wireless Location System uses a network of calibration transmitters whose signal characteristics match those of the target wireless

- transmitters. These calibration transmitters may be ordinary wireless telephones emitting periodic registration signals and/or page response signals. Each usable SCS-to-SCS baseline is preferably calibrated periodically using a calibration transmitter that has a relatively clear and unobstructed path to both SCS's 10 associated with the baseline. The calibration signal is processed identically to a signal from a target wireless transmitter. Since the TDOA values are known *a priori*, any errors in the calculations are due to systemic errors in the Wireless Location System. These systemic errors can then be removed in the subsequent location calculations for target transmitters.
- Figure 2G illustrates the external calibration method for minimizing timing errors. As shown, a first SCS 10A at a point "A" and a second SCS 10A at a point "B" have an associated baseline A-B. A calibration signal emitted at time T_0 by a calibration transmitter at point "C" will theoretically reach first SCS 10A at time $T_0 + T_{AC}$. T_{AC} is a measure of the amount of time required for the calibration signal to travel from the antenna on the calibration transmitter to the dual port digital memory in a digital receiver. Likewise, the same calibration signal will reach second SCS 10B at a theoretical time $T_0 + T_{BC}$. Usually, however, the calibration signal will not reach the digital memory and the digital signal processing components of the respective SCS's 10 at exactly the correct times. Rather, there will be errors e_1 and e_2 in the amount of time (T_{AC} , T_{BC}) it takes the calibration signal to propagate from the calibration transmitter to the SCS's 10, respectively, such that the exact times of arrival are actually $T_0 + T_{AC} + e_1$ and $T_0 + T_{BC} + e_2$. Such errors will be due to some extent to delays in the signal propagation through the air, i.e., from the calibration transmitter's antenna to the SCS antennas; however, the errors will be due primarily to time varying characteristics in the SCS front end components. The errors e_1 and e_2 cannot be determined *per se* because the system does not know the exact time (T_0) at which the calibration signal was transmitted. The system can, however, determine the error in the *difference* in the time of arrival of the calibration signal at the respective SCS's 10 of any given pair of SCS's 10. This TDOA error value is defined as the difference between the measured TDOA value and the theoretical TDOA value τ_0 , wherein τ_0 is the theoretical differences between the theoretical delay values T_{AC} and T_{BC} . Theoretical TDOA values for each pair of SCS's

10 and each calibration transmitter are known because the positions of the SCS's 10 and calibration transmitter, and the speed at which the calibration signal propagates, are known. The measured TDOA baseline (TDOA_{A-B}) can be represented as TDOA_{A-B} = τ_0 + ϵ , wherein $\epsilon = e_1 - e_2$. In a similar manner, a calibration signal from a second
 5 calibration transmitter at point "D" will have associated errors e_3 and e_4 . The ultimate value of ϵ to be subtracted from TDOA measurements for a target transmitter will be a function (e.g., weighted average) of the ϵ values derived for one or more calibration transmitters. Therefore, a given TDOA measurement (TDOA_{measured}) for a pair of SCS's 10 at points "X" and "Y" and a target wireless transmitter at an unknown location will be
 10 corrected as follows:

$$\begin{aligned} \text{TDOA}_{X-Y} &= \text{TDOA}_{\text{measured}} - \epsilon \\ \epsilon &= k_1\epsilon_1 + k_2\epsilon_2 + \dots k_N\epsilon_N, \end{aligned}$$

15 where k_1, k_2 , etc., are weighting factors and ϵ_1, ϵ_2 , etc., are the errors determined by subtracting the measured TDOA values from the theoretical values for each calibration transmitter. In this example, error value ϵ_1 may be the error value associated with the calibration transmitter at point "C" in the drawing. The weighting factors are determined by the operator of the Wireless Location System, and input into the configuration tables
 20 for each baseline. The operator will take into consideration the distance from each calibration transmitter to the SCS's 10 at points "X" and "Y", the empirically determined line of sight from each calibration transmitter to the SCS's 10 at points "X" and "Y", and the contribution that each SCS "X" and "Y" would have made to a location estimate of a wireless transmitter that might be located in the vicinity of each calibration transmitter.
 25 In general, calibration transmitters that are nearer to the SCS's 10 at points "X" and "Y" will be weighted higher than calibration transmitters that are farther away, and calibration transmitters with better line of sight to the SCS's 10 at points "X" and "Y" will be weighted higher than calibration transmitters with worse line of sight.
 30 Each error component e_1, e_2 , etc., and therefore the resulting error component ϵ , can vary widely, and wildly, over time because some of the error component is due to

5 multipath reflection from the calibration transmitter to each SCS 10. The multipath reflection is very much path dependent and therefore will vary from measurement to measurement and from path to path. It is not an object of this method to determine the multipath reflection for these calibration paths, but rather to determine the portion of the errors that are attributable to the components of the SCS's 10. Typically, therefore, error values e_1 and e_3 will have a common component since they relate to the same first SCS 10A. Likewise, error values e_2 and e_4 will also have a common component since they relate to the second SCS 10B. It is known that while the multipath components can vary wildly, the component errors vary slowly and typically vary sinusoidally. Therefore, in 10 the external calibration method, the error values ϵ are filtered using a weighted, time-based filter that decreases the weight of the wildly varying multipath components while preserving the relatively slow changing error components attributed to the SCS's 10. One such exemplary filter used in the external calibration method is the Kalman filter.

15 The period between calibration transmissions is varied depending on the error drift rates determined for the SCS components. The period of the drift rate should be much longer than the period of the calibration interval. The Wireless Location System monitors the period of the drift rate to determine continuously the rate of change, and may periodically adjust the calibration interval, if needed. Typically, the calibration rate for a 20 Wireless Location System such as one in accordance with the present invention is between 10 and 30 minutes. This corresponds well with the typical time period for the registration rate in a wireless communications system. If the Wireless Location System were to determine that the calibration interval must be adjusted to a rate faster than the registration rate of the wireless communications system, then the AP 14 (Figure 1) would 25 automatically force the calibration transmitter to transmit by paging the transmitter at the prescribed interval. Each calibration transmitter is individually addressable and therefore the calibration interval associated with each calibration transmitter can be different.

Since the calibration transmitters used in the external calibration method are standard 30 telephones, the Wireless Location System must have a mechanism to distinguish those telephones from the other wireless transmitters that are being located for various

application purposes. The Wireless Location System maintains a list of the identities of the calibration transmitters, typically in the TLP 12 and in the AP 14. In a cellular system, the identity of the calibration transmitter can be the Mobile Identity Number, or MIN. When the calibration transmitter makes a transmission, the transmission is received
5 by each SCS 10 and demodulated by the appropriate SCS 10. The Wireless Location System compares the identity of the transmission with a pre-stored tasking list of identities of all calibration transmitters. If the Wireless Location System determines that the transmission was a calibration transmission, then the Wireless Location System initiates external calibration processing.

10

Internal Calibration Method

In addition to the external calibration method, it is an object of the present invention to calibrate all channels of the wideband digital receiver used in the SCS 10 of a Wireless Location System. The external calibration method will typically calibrate only
15 a single channel of the multiple channels used by the wideband digital receiver. This is because the fixed calibration transmitters will typically scan to the highest-power control channel, which will typically be the same control channel each time. The transfer function of a wideband digital receiver, along with the other associated components, does not remain perfectly constant, however, and will vary with time and temperature.
20 Therefore, even though the external calibration method can successfully calibrate a single channel, there is no assurance that the remaining channels will also be calibrated.

The internal calibration method, represented in the flowchart of Figure 2H, is particularly suited for calibrating an individual first receiver system (i.e., SCS 10) that is
25 characterized by a time- and frequency-varying transfer function, wherein the transfer function defines how the amplitude and phase of a received signal will be altered by the receiver system and the receiver system is utilized in a location system to determine the location of a wireless transmitter by, in part, determining a difference in time of arrival of a signal transmitted by the wireless transmitter and received by the receiver system to
30 be calibrated and another receiver system, and wherein the accuracy of the location estimate is dependent, in part, upon the accuracy of TDOA measurements made by the system. An example of a AMPS RCC transfer function is depicted in Figure 2I, which

depicts how the phase of the transfer function varies across the 21 control channels spanning 630 KHz.

Referring to Figure 2H, the internal calibration method includes the steps of temporarily
5 and electronically disconnecting the antenna used by a receiver system from the receiver system (step S-20); injecting an internally generated wideband signal with known and stable signal characteristics into the first receiver system (step S-21); utilizing the generated wideband signal to obtain an estimate of the manner in which the transfer function varies across the bandwidth of the first receiver system (step S-22); and utilizing
10 the estimate to mitigate the effects of the variation of the first transfer function on the time and frequency measurements made by the first receiver system (step S-23). One example of a stable wideband signal used for internal calibration is a comb signal, which is comprised of multiple individual, equal-amplitude frequency elements at a known spacing, such as 5 KHz. An example of such a signal is shown in Figure 2I.

15 The antenna must be temporarily disconnected during the internal calibration process to prevent external signals from entering the wideband receiver and to guarantee that the receiver is only receiving the stable wideband signal. The antenna is electronically disconnected only for a few milliseconds to minimize the chance of missing too much of
20 a signal from a wireless transmitter. In addition, internal calibration is typically performed immediately after external calibration to minimize the possibility that the any component in the SCS 10 drifts during the interval between external and internal calibration. The antenna is disconnected from the wideband receiver using two electronically controlled RF relays (not shown). An RF relay cannot provide perfect
25 isolation between input and output even when in the "off" position, but it can provide up to 70 dB of isolation. Two relays may be used in series to increase the amount of isolation and to further assure that no signal is leaked from the antenna to the wideband receiver during calibration. Similarly, when the internal calibration function is not being used, the internal calibration signal is turned off, and the two RF relays are also turned
30 off to prevent leakage of the internal calibration signals into the wideband receiver when the receiver is collecting signals from wireless transmitters.

The external calibration method provides an absolute calibration of a single channel and the internal calibration method then calibrates each other channel relative to the channel that had been absolutely calibrated. The comb signal is particularly suited as a stable wideband signal because it can be easily generated using a stored replica of the signal
5 and a digital to analog converter.

External Calibration Using Wideband Calibration Signal

The external calibration method described next may be used in connection with an SCS receiver system characterized by a time- and frequency-varying transfer
10 function, which preferably includes the antennas, filters, amplifiers, duplexors, multi-couplers, splitters, and cabling associated with the SCS receiver system. The method includes the step of transmitting a stable, known wideband calibration signal from an external transmitter. The wideband calibration signal is then used to estimate the transfer function across a prescribed bandwidth of the SCS receiver system. The estimate of the
15 transfer function is subsequently employed to mitigate the effects of variation of the transfer function on subsequent TDOA/FDOA measurements. The external transmission is preferably of short duration and low power to avoid interference with the wireless communications system hosting the Wireless Location System.

20 In the preferred method, the SCS receiver system is synchronized with the external transmitter. Such synchronization may be performed using GPS timing units. Moreover, the receiver system may be programmed to receive and process the entire wideband of the calibration signal only at the time that the calibration signal is being sent. The receiver system will not perform calibration processing at any time other than when in
25 synchronization with the external calibration transmissions. In addition, a wireless communications link is used between the receiver system and the external calibration transmitter to exchange commands and responses. The external transmitter may use a directional antenna to direct the wideband signal only at the antennas of the SCS receiver system. Such as directional antenna may be a Yagi antenna (i.e. linear end-fire array).

30 The calibration method preferably includes making the external transmission only when the directional antenna is aimed at the receiver system's antennas and the risk of multipath reflection is low.

Calibrating for Station Biases

Another aspect of the present invention concerns a calibration method to correct for station biases in a SCS receiver system. The “station bias” is defined as the finite
5 delay between when an RF signal from a wireless transmitter reaches the antenna and when that same signal reached the wideband receiver. The inventive method includes the step of measuring the length of the cable from the antennas to the filters and determining the corresponding delays associated with the cable length. In addition, the method includes injecting a known signal into the filter, duplexor, multi-coupler, or RF splitter
10 and measuring the delay and phase response versus frequency response from the input of each device to the wideband receiver. The delay and phase values are then combined and used to correct subsequent location measurements. When used with the GPS based timing generation described above, the method preferably includes correcting for the GPS cable lengths. Moreover, an externally generated reference signal is preferably used
15 to monitor changes in station bias that may arise due to aging and weather. Finally, the station bias by RF channel and for each receiver system in the Wireless Location System is preferably stored in tabular form in the Wireless Location System for use in correcting subsequent location processing.

20 Performance Monitoring

The Wireless Location System uses methods similar to calibration for performance monitoring on a regular and ongoing basis. These methods are depicted in the flowcharts of Figure 2K and 2L. Two methods of performance monitoring are used: fixed phones and drive testing of surveyed points. The fixed phone method comprises the
25 following steps (see Figure 2K):

- standard wireless transmitters are permanently placed at various points within the coverage area of the Wireless Location System (these are then known as the fixed phones) (step S-30);
- the points at which the fixed phones have been placed are surveyed so that their
30 location is precisely known to within a predetermined distance, for example ten feet (step S-31);
- the surveyed locations are stored in a table in the AP 14 (step S-32);

the fixed phones are permitted to register on the wireless communications system, at the rate and interval set by the wireless communications system for all wireless transmitters on the system (step S-33);

at each registration transmission by a fixed phone, the Wireless Location System
5 locates the fixed phone using normal location processing (as with the calibration transmitters, the Wireless Location System can identify a transmission as being from a fixed phone by storing the identities in a table) (step S-34);

the Wireless Location System computes an error between the calculated location determined by the location processing and the stored location determined by
10 survey (step S-35);

the location, the error value, and other measured parameters are stored along with a time stamp in a database in the AP 14 (step S-36);

the AP 14 monitors the instant error and other measured parameters (collectively referred to as an extended location record) and additionally computes various

15 statistical values of the error(s) and other measured parameters (step S-37); and if any of the error or other values exceed a pre-determined threshold or a historical statistical value, either instantaneously or after performing statistical filtering over a prescribed number of location estimates, the AP 14 signals an alarm to the operator of the Wireless Location System (step S-38).

20

The extended location record includes a large number of measured parameters usefully for analyzing the instant and historical performance of the Wireless Location System.

These parameters include: the RF channel used by the wireless transmitter, the antenna port(s) used by the Wireless Location System to demodulate the wireless transmission,

25 the antenna ports from which the Wireless Location System requested RF data, the peak, average, and variance in power of the transmission over the interval used for location

processing, the SCS 10 and antenna port chosen as the reference for location processing, the correlation value from the cross-spectra correlation between every other SCS 10 and antenna used in location processing and the reference SCS 10 and antenna, the delay

30 value for each baseline, the multipath mitigation parameters, and the residual values remaining after the multipath mitigation calculations. Any of these measured parameters can be monitored by the Wireless Location System for the purpose of determining how

the Wireless Location System is performing. One example of the type of monitoring performed by the Wireless Location System may be the variance between the instant value of the correlation on a baseline and the historical range of the correlation value. Another may be the variance between the instant value of the received power at a particular antenna and the historical range of the received power. Many other statistical values can be calculated and this list is not exhaustive.

The number of fixed phones placed into the coverage area of the Wireless Location System can be determined based upon the density of the cell sites, the difficulty of the terrain, and the historical ease with which wireless communications systems have performed in the area. Typically the ratio is about one fixed phone for every six cell sites, however in some areas a ratio of one to one may be required. The fixed phones provide a continuous means to monitor the performance of the Wireless Location System, as well as the monitor any changes in the frequency plan that the carrier may have made. Many times, changes in the frequency plan will cause a variation in the performance of the Wireless Location System and the performance monitoring of the fixed phones provide an immediate indication to the Wireless Location System operator.

Drive testing of surveyed points is very similar to the fixed phone monitoring. Fixed phones typically can only be located indoors where access to power is available (i.e. the phones must be continuously powered on to be effective). To obtain a more complete measurement of the performance of the location performance, drive testing of outdoor test points is also performed. Referring to Figure 2L, as with the fixed phones, prescribed test points throughout the coverage area of the Wireless Location System are surveyed to within ten feet (step S-40). Each test point is assigned a code, wherein the code consists of either a "*" or a "#", followed by a sequence number (step S-41). For example, "*1001" through "*1099" may be a sequence of 99 codes used for test points. These codes should be sequences, that when dialed, are meaningless to the wireless communications system (i.e. the codes do not cause a feature or other translation to occur in the MSC, except for an intercept message). The AP 14 stores the code for each test point along with the surveyed location (step S-42). Subsequent to these initial steps, any wireless transmitter dialing any of the codes will be triggered and located using normal

location processing (steps S-43 and S-44). The Wireless Location System automatically computes an error between the calculated location determined by the location processing and the stored location determined by survey, and the location and the error value are stored along with a time stamp in a database in the AP 14 (steps S-45 and S-46). The AP
5 14 monitors the instant error, as well as various historical statistical values of the error. If the error values exceed a pre-determined threshold or a historical statistical value, either instantaneously or after performing statistical filtering over a prescribed number of location estimates, the AP 14 signals an alarm to the operator of the Wireless Location System (step S-47).

10

TDOA Location Processor (TLP)

The TLP 12, depicted in Figures 1, 1A and 3, is a centralized digital signal processing system that manages many aspects of the Wireless Location System, especially the SCS's 10, and provides control over the location processing. Because
15 location processing is DSP intensive, one of the major advantages of the TLP 12 is that the DSP resources can be shared among location processing initiated by transmissions at any of the SCS's 10 in a Wireless Location System. That is, the additional cost of DSP's at the SCS's 10 is reduced by having the resource centrally available. As shown in Figure 3, there are three major components of the TLP 12: DSP modules 12-1, T1/E1
20 communications modules 12-2 and a controller module 12-3.

The T1/E1 communications modules 12-2 provide the communications interface to the SCS's 10 (T1 and E1 are standard communications speeds available throughout the world). Each SCS 10 communicates to a TLP 12 using one or more DS0's (which are
25 typically 56Kbps or 64 Kbps). Each SCS 10 typically connects to a fractional T1 or E1 circuit, using, e.g., a drop and insert unit or channel bank at the cell site. Frequently, this circuit is shared with the base station, which communicates with the MSC. At a central site, the DS0's assigned to the base station are separated from the DS0's assigned to the SCS's 10. This is typically accomplished external to the TLP 12 using a digital access
30 and control system (DACS) 13A that not only separates the DS0's but also grooms the DS0's from multiple SCS's 10 onto full T1 or E1 circuits. These circuits then connect from the DACS 13A to the DACS 13B and then to the T1/E1 communications module

on the TLP 12. Each T1/E1 communications module contains sufficient digital memory to buffer packets of data to and from each SCS 10 communicating with the module. A single TLP chassis may support one or more T1/E1 communications modules.

- 5 The DSP modules 12-1 provide a pooled resource for location processing. A single module may typically contain two to eight digital signal processors, each of which are equally available for location processing. Two types of location processing are supported: central based and station based, which are described in further detail below. The TLP controller 12-3 manages the DSP module(s) 12-1 to obtain optimal throughput.
- 10 Each DSP module contains sufficient digital memory to store all of the data necessary for location processing. A DSP is not engaged until all of the data necessary to begin location processing has been moved from each of the involved SCS's 10 to the digital memory on the DSP module. Only then is a DSP given the specific task to locate a specific wireless transmitter. Using this technique, the DSP's , which are an expensive
- 15 resource, are never kept waiting. A single TLP chassis may support one or more DSP modules.

- The controller module 12-3 provides the real time management of all location processing within the Wireless Location System. The AP 14 is the top-level management entity
- 20 within the Wireless Location System, however its database architecture is not sufficiently fast to conduct the real time decision making when transmissions occur. The controller module 12-3 receives messages from the SCS's 10, including: status, spectral energy in various channels for various antennas, demodulated messages, and diagnostics. This enables the controller to continuously determine events occurring in the Wireless
- 25 Location System, as well as to send commands to take certain actions. When a controller module receives demodulated messages from SCS's 10, the controller module decides whether location processing is required for a particular wireless transmission. The controller module 12-3 also determines which SCS's 10 and antennas to use in location processing, including whether to use central based or station based location processing.
- 30 The controller module commands SCS's 10 to return the necessary data, and commands the communications modules and DSP modules to sequentially perform their necessary roles in location processing. These steps are described below in further detail.

The controller module 12-3 maintains a table known as the Signal of Interest Table (SOIT). This table contains all of the criteria that may be used to trigger location processing on a particular wireless transmission. The criteria may include, for example, the Mobile Identity Number, the Mobile Station ID, the Electronic Serial Number, dialed digits, System ID, RF channel number, cell site number or sector number, type of transmission, and other types of data elements. Some of the trigger events may have higher or lower priority levels associated with them for use in determining the order of processing. Higher priority location triggers will always be processing before lower priority location triggers. However, a lower priority trigger that has already begun location processing will complete the processing before being assigned to a higher priority task. The master Tasking List for the Wireless Location System is maintained on the AP 14, and copies of the Tasking List are automatically downloaded to the Signal of Interest Table in each TLP 12 in the Wireless Location System. The full Signal of Interest Table is downloaded to a TLP 12 when the TLP 12 is reset or first starts. Subsequent to those two events, only changes are downloaded from the AP 14 to each TLP 12 to conserve communications bandwidth. The TLP 12 to AP 14 communications protocol preferably contains sufficient redundancy and error checking to prevent incorrect data from ever being entered into the Signal of Interest Table. When the AP 14 and TLP 12 periodically have spare processing capacity available, the AP 14 reconfirms entries in the Signal of Interest Table to ensure that all Signal of Interest Table entries in the Wireless Location System are in full synchronization.

Each TLP chassis has a maximum capacity associated with the chassis. For example, a single TLP chassis may only have sufficient capacity to support between 48 and 60 SCS's 10. When a wireless communications system is larger than the capacity of a single TLP chassis, multiple TLP chassis are connected together using Ethernet networking. The controller module 12-3 is responsible for inter-TLP communications and networking, and communicates with the controller modules in other TLP chassis and with Application Processors 14 over the Ethernet network. Inter-TLP communications is required when location processing requires the use of SCS's 10 that are connected to different TLP chassis. Location processing for each wireless transmission is assigned to a

single DSP module in a single TLP chassis. The controller modules 12-3 in TLP chassis select the DSP module on which to perform location processing, and then route all of the RF data used in location processing to that DSP module. If RF data is required from the SCS's 10 connected to more than one TLP 12, then the controller modules in all
5 necessary TLP chassis communicate to move the RF data from all necessary SCS's 10 to their respective connected TLP's 12 and then to the DSP module and TLP chassis assigned to the location processing. The controller module supports two fully independent Ethernet networks for redundancy. A break or failure in any one network causes the affected TLP's 12 to immediately shift all communications to the other
10 network.

The controller modules 12-3 maintain a complete network map of the Wireless Location System, including the SCS's 10 associated with each TLP chassis. The network map is a table stored in the controller module containing a list of the candidate SCS/antennas that
15 may be used in location processing, and various parameters associated with each of the SCS/antennas. The structure of an exemplary network map is depicted in Figure 3A. There is a separate entry in the table for each antenna connected to an SCS 10. When a wireless transmission occurs in an area that is covered by SCS's 10 communicating with more than one TLP chassis, the controller modules in the involved TLP chassis
20 determine which TLP chassis will be the "master" TLP chassis for the purpose of managing location processing. Typically, the TLP chassis associated with the SCS 10 that has the primary channel assignment for the wireless transmission is assigned to be the master. However, another TLP chassis may be assigned instead if that TLP temporarily has no DSP resources available for location processing, or if most of the
25 SCS's 10 involved in location processing are connected to another TLP chassis and the controller modules are minimizing inter-TLP communications. This decision making process is fully dynamic, but is assisted by tables in the TLP 12 that pre-determine the preferred TLP chassis for every primary channel assignment. The tables are created by the operator of the Wireless Location System, and programmed using the Network
30 Operations Console.

The networking described herein functions for both TLP chassis associated with the same wireless carrier, as well as for chassis that overlap or border the coverage area between two wireless carriers. Thus it is possible for a TLP 12 belonging to a first wireless carrier to be networked and therefore receive RF data from a TLP 12 (and the SCS's 10 associated with that TLP 12) belonging to a second wireless carrier. This networking is particularly valuable in rural areas, wherein the performance of the Wireless Location System can be enhanced by deploying SCS's 10 at cell sites of multiple wireless carriers. Since in many cases wireless carriers do not colocate cell sites, this feature enables the Wireless Location System to access more geographically diverse antennas than might be available if the Wireless Location System used only the cell sites from a single wireless carrier. As described below, the proper selection and use of antennas for location processing can enhance the performance of the Wireless Location System.

The controller module 12-3 passes many messages, including location records, to the AP 14, many of which are described below. Usually, however, demodulated data is not passed from the TLP 12 to the AP 14. If, however, the TLP 12 receives demodulated data from a particular wireless transmitter and the TLP 12 identifies the wireless transmitter as being a registered customer of a second wireless carrier in a different coverage area, the TLP 12 may pass the demodulated data to the first (serving) AP 14A. This will enable the first AP 14A to communicate with a second AP 14B associated with the second wireless carrier, and determine whether the particular wireless transmitter has registered for any type of location services. If so, the second AP 14B may instruct the first AP 14A to place the identity of the particular wireless transmitter into the Signal of Interest Table so that the particular wireless transmitter will be located for as long as the particular wireless transmitter is in the coverage area of the first Wireless Location System associated with the first AP 14A. When the first Wireless Location System has detected that the particular wireless transmitter has not registered in a time period exceeding a pre-determined threshold, the first AP 14A may instruct the second AP 14B that the identity of the particular wireless transmitter is being removed from the Signal of Interest Table for the reason of no longer being present in the coverage area associated with the first AP 14A.

Diagnostic Port

The TLP 12 supports a diagnostic port that is highly useful in the operation and diagnosis of problems within the Wireless Location System. This diagnostic port can be accessed either locally at a TLP 12 or remotely over the Ethernet network connecting the TLP's 12 to the AP's. The diagnostic port enables an operator to write to a file all of the demodulation and RF data received from the SCS's 10, as well as the intermediate and final results of all location processing. This data is erased from the TLP 12 after processing a location estimate, and therefore the diagnostic port provides the means to save the data for later post-processing and analysis. The inventor's experience in operating large scale wireless location systems is that a very small number of location estimates can occasionally have very large errors, and these large errors can dominate the overall operating statistics of the Wireless Location System over any measurement period. Therefore, it is important to provide the operator with a set of tools that enable the Wireless Location System to detect and trap the cause of the very large errors to diagnose and mitigate those errors. The diagnostic port can be set to save the above information for all location estimates, for location estimates from particular wireless transmitters or at particular test points, or for location estimates that meet a certain criteria. For example, for fixed phones or drive testing of surveyed points, the diagnostic port can determine the error in the location estimate in real time and then write the above described information only for those location estimates whose error exceeds a predetermined threshold. The diagnostic port determines the error in real time by storing the surveyed latitude, longitude coordinate of each fixed phone and drive test point in a table, and then calculating a radial error when a location estimate for the corresponding test point is made.

Redundancy

The TLP's 12 implement redundancy using several inventive techniques, allowing the Wireless Location System to support an M plus N redundancy method. M plus N redundancy means that N redundant (or standby) TLP chassis are used to provide full redundant backup to M online TLP chassis. For example, M may be ten and N may be two.

First, the controller modules in different TLP chassis continuously exchange status and “heartbeat” messages at pre-determined time intervals between themselves and with every AP 14 assigned to monitor the TLP chassis. Thus, every controller module has continuous and full status of every other controller module in the Wireless Location System. The controller modules in different TLP chassis periodically select one controller module in one TLP 12 to be the master controller for a group of TLP chassis. The master controller may decide to place a first TLP chassis into off-line status if the first TLP 12A reports a failed or degraded condition in its status message, or if the first TLP 12A fails to report any status or heartbeat messages within its assigned and pre-determined time. If the master controller places a first TLP 12A into off-line status, the master controller may assign a second TLP 12B to perform a redundant switchover and assume the tasks of the off-line first TLP 12A. The second TLP 12B is automatically sent the configuration that had been loaded into the first TLP 12A; this configuration may be downloaded from either the master controller or from an AP 14 connected to the TLP’s 12. The master controller may be a controller module on any one of the TLP’s 12 that is not in off-line status, however there is a preference that the master controller be a controller module in a stand-by TLP 12. When the master controller is the controller module in a stand-by TLP 12, the time required to detect a failed first TLP 12A, place the first TLP 12A into off-line status, and then perform a redundant switchover can be accelerated.

Second, all of the T1 or E1 communications between the SCS’s 10 and each of the TLP T1/E1 communications modules 12-2 are preferably routed through a high-reliability DACS that is dedicated to redundancy control. The DACS 13B is connected to every groomed T1/E1 circuit containing DS0’s from SCS’s 10 and is also connected to every T1/E1 communications module 12-2 of every TLP 12. Every controller module at every TLP 12 contains a map of the DACS 13B that describes the DACS’ connection list and port assignments. This DACS 13B is connected to the Ethernet network described above and can be controlled by any of the controller modules 12-3 at any of the TLP’s 12. When a second TLP 12 is placed into off-line status by a master controller, the master controller sends commands to the DACS 13B to switch the groomed T1/E1 circuit

communicating with the first TLP 12A to a second TLP 12B which had been in standby status. At the same time, the AP 14 downloads the complete configuration file that was being used by the second (and now off-line) TLP 12B to the third (and now online) TLP 12C. The time from the first detection of a failed first TLP chassis to the complete
5 switch-over and assumption of processing responsibilities by a third TLP chassis is typically less than few seconds. In many cases, no RF data is lost by the SCS's 10 associated with the failed first TLP chassis, and location processing can continue without interruption. At the time of a TLP fail-over when a first TLP 12A is placed into off-line status, the NOC 16 creates an alert to notify the Wireless Location System operator that
10 the event has occurred.

Third, each TLP chassis contains redundant power supplies, fans, and other components. A TLP chassis can also support multiple DSP modules, so that the failure of a single DSP module or even a single DSP on a DSP module reduces the overall amount of
15 processing resources available but does not cause the failure of the TLP chassis. In all of the cases described in this paragraph, the failed component of the TLP 12 can be replaced without placing the entire TLP chassis into off-line status. For example, if a single power supply fails, the redundant power supply has sufficient capacity to singly support the load of the chassis. The failed power supply contains the necessary circuitry
20 to remove itself from the load of the chassis and not cause further degradation in the chassis. Similarly, a failed DSP module can also remove itself from the active portions of the chassis, so as to not cause a failure of the backplane or other modules. This enables the remainder of the chassis, including the second DSP module, to continue to function normally. Of course, the total processing throughput of the chassis is reduced but a total
25 failure is avoided.

Application Processor (AP) 14

The AP 14 is a centralized database system, comprising a number of software processes that manage the entire Wireless Location System, provide interfaces to
30 external users and applications, store location records and configurations, and support various application-related functionality. The AP 14 uses a commercial hardware platform that is sized to match the throughput of the Wireless Location System. The AP

14 also uses a commercial relational database system (RDBMS), which has been significantly customized to provide the functionality described herein. While the SCS 10 and TLP 12 preferably operate together on a purely real time basis to determine location and create location records, the AP 14 can operate on both a real time basis to store and forward location records and a non-real time basis to post-process location records and provide access and reporting over time. The ability to store, retrieve, and post-process location records for various types of system and application analysis has proven to be a powerful advantage of the present invention. The main collection of software processes is known as the ApCore, which is shown in Figure 4 and includes the following functions:

The AP Performance Guardian (ApPerfGuard) is a dedicated software process that is responsible for starting, stopping, and monitoring most other ApCore processes as well as ApCore communications with the NOC 16. Upon receiving a configuration update command from the NOC, ApPerfGuard updates the database and notifies all other processes of the change. ApPerfGuard starts and stops appropriate processes when the NOC directs the ApCore to enter specific run states, and constantly monitors other software processes scheduled to be running to restart them if they have exited or stopping and restarting any process that is no longer properly responding. ApPerfGuard is assigned to one of the highest processing priorities so that this process cannot be blocked by another process that has "run away". ApPerfGuard is also assigned dedicated memory that is not accessible by other software processes to prevent any possible corruption from other software processes.

The AP Dispatcher (ApMnDsptch) is a software process that receives location records from the TLP's 12 and forwards the location records to other processes. This process contains a separate thread for each physical TLP 12 configured in the system, and each thread receives location records from that TLP 12. For system reliability, the ApCore maintains a list containing the last location record sequence number received from each TLP 12, and sends this sequence number to the TLP 12 upon initial connection. Thereafter, the AP 14 and the TLP 12 maintain a protocol whereby the TLP 12 sends

each location record with a unique identifier. ApMnDsptch forwards location records to multiple processes, including Ap911, ApDbSend, ApDbRecvLoc, and ApDbFileRecv.

- The AP Tasking Process (ApDbSend) controls the Tasking List within the Wireless Location System. The Tasking List is the master list of all of the trigger criteria that determines which wireless transmitters will be located, which applications created the criteria, and which applications can receive location record information. The ApDbSend process contains a separate thread for each TLP 12, over which the ApDbSend synchronizes the Tasking List with the Signal of Interest Table on each TLP 12.
- 10 ApDbSend does not send application information to the Signal of Interest Table, only the trigger criteria. Thus the TLP 12 does not know why a wireless transmitter must be located. The Tasking List allows wireless transmitters to be located based upon Mobile Identity Number (MIN), Mobile Station Identifier (MSID), Electronic Serial Number (ESN) and other identity numbers, dialed sequences of characters and / or digits, home
- 15 System ID (SID), originating cell site and sector, originating RF channel, or message type. The Tasking List allows multiple applications to receive location records from the same wireless transmitter. Thus, a single location record from a wireless transmitter that has dialed "911" can be sent, for example, to a 911 PSAP, a fleet management application, a traffic management application, and to an RF optimization application.
- 20
- The Tasking List also contains a variety of flags and field for each trigger criteria, some of which are described elsewhere in this specification. One flag, for example, specifies the maximum time limit before which the Wireless Location System must provide a rough or final estimate of the wireless transmitter. Another flag allows location
- 25 processing to be disabled for a particular trigger criteria such as the identity of the wireless transmitter. Another field contains the authentication required to make changes to the criteria for a particular trigger; authentication enables the operator of the Wireless Location System to specify which applications are authorized to add, delete, or make changes to any trigger criteria and associated fields or flags. Another field contains the
- 30 Location Grade of Service associated with the trigger criteria; Grade of Service indicates to the Wireless Location System the accuracy level and priority level desired for the location processing associated with a particular trigger criteria. For example, some

applications may be satisfied with a rough location estimate (perhaps for a reduced location processing fee), while other applications may be satisfied with low priority processing that is not guaranteed to complete for any given transmission (and which may be pre-empted for high priority processing tasks). The Wireless Location System also includes means to support the use of wildcards for trigger criteria in the Tasking List. For example, a trigger criteria can be entered as "MIN = 215555****". This will cause the Wireless Location System to trigger location processing for any wireless transmitter whose MIN begins with the six digits 215555 and ends with any following four digits. The wildcard characters can be placed into any position in a trigger criteria. This feature can save on the number of memory locations required in the Tasking List and Signal of Interest Table by grouping blocks of related wireless transmitters together.

ApDbSend also supports dynamic tasking. For example, the MIN, ESN, MSID, or other identity of any wireless transmitter that has dialed "911" will automatically be placed onto the Tasking List by ApDbSend for one hour. Thus, any further transmissions by the wireless transmitter that dialed "911" will also be located in case of further emergency. For example, if a PSAP calls back a wireless transmitter that had dialed "911" within the last hour, the Wireless Location System will trigger on the page response message from the wireless transmitter, and can make this new location record available to the PSAP. This dynamic tasking can be set for any interval of time after an initiation event, and for any type of trigger criteria. The ApDbSend process is also a server for receiving tasking requests from other applications. These applications, such as fleet management, can send tasking requests via a socket connection, for example. These applications can either place or remove trigger criteria. ApDbSend conducts an authentication process with each application to verify that that the application has been authorized to place or remove trigger criteria, and each application can only change trigger criteria related to that application.

The AP 911 Process (Ap911) manages each interface between the Wireless Location System and E9-1-1 network elements, such as tandem switches, selective routers, ALI databases and/or PSAPs. The Ap911 process contains a separate thread for each connection to a E9-1-1 network element, and can support more than one thread to each

network element. The Ap911 process can simultaneously operate in many modes based upon user configuration, and as described herein. The timely processing of E9-1-1 location records is one of the highest processing priorities in the AP 14, and therefore the Ap911 executes entirely out of random access memory (RAM) to avoid the delay associated with first storing and then retrieving a location record from any type of disk. When ApMnDsptch forwards a location record to Ap911, Ap911 immediately makes a routing determination and forwards the location record over the appropriate interface to a E9-1-1 network element. A separate process, operating in parallel, records the location record into the AP 14 database.

10

The AP 14, through the Ap911 process and other processes, supports two modes of providing location records to applications, including E9-1-1: "push" and "pull" modes. Applications requesting push mode receive a location record as soon as it is available from the AP 14. This mode is especially effective for E9-1-1 which has a very time

critical need for location records, since E9-1-1 networks must route wireless 9-1-1 calls to the correct PSAP within a few seconds after a wireless caller has dialed "911".

Applications requesting pull mode do not automatically receive location records, but rather must send a query to the AP 14 regarding a particular wireless transmitter in order to receive the last, or any other location record, about the wireless transmitter. The query from the application can specify the last location record, a series of location records, or all location records meeting a specific time or other criteria, such as type of transmission. An example of the use of pull mode in the case of a "911" call is the E9-1-1 network first receiving the voice portion of the "911" call and then querying the AP 14 to receive the location record associated with that call.

25

When the Ap911 process is connected to many E9-1-1 networks elements, Ap911 must determine to which E9-1-1 network element to push the location record (assuming that "push" mode has been selected). The AP 14 makes this determination using a dynamic routing table. The dynamic routing table is used to divide a geographic region into cells.

Each cell, or entry, in the dynamic routing table contains the routing instructions for that cell. It is well known that one minute of latitude is 6083 feet, which is about 365 feet per millidegree. Additionally, one minute of longitude is cosine(latitude) times 6083 feet,

which for the Philadelphia area is about 4659 feet, or about 280 feet per millidegree. A table of size one thousand by one thousand, or one million cells, can contain the routing instructions for an area that is about 69 miles by 53 miles, which is larger than the area of Philadelphia in this example, and each cell could contain a geographic area of 365 feet
5 by 280 feet. The number of bits allocated to each entry in the table must only be enough to support the maximum number of routing possibilities. For example, if the total number of routing possibilities is sixteen or less, then the memory for the dynamic routing table is one million times four bits, or one-half megabyte. Using this scheme, an area the size of Pennsylvania could be contained in a table of approximately twenty megabytes or
10 less, with ample routing possibilities available. Given the relatively inexpensive cost of memory, this inventive dynamic routing table provides the AP 14 with a means to quickly push the location records for "911" calls only to the appropriate E9-1-1 network element.

15 The AP 14 allows each entry in dynamic routing to be populated using manual or automated means. Using the automated means, for example, an electronic map application can create a polygon definition of the coverage area of a specific E9-1-1 network element, such as a PSAP. The polygon definition is then translated into a list of latitude, longitude points contained within the polygon. The dynamic routing table cell
20 corresponding to each latitude, longitude point is then given the routing instruction for that E9-1-1 network element that is responsible for that geographic polygon.

When the Ap911 process receives a "911" location record for a specific wireless transmitter, Ap911 converts the latitude, longitude into the address of a specific cell in
25 the dynamic routing table. Ap911 then queries the cell to determine the routing instructions, which may be push or pull mode and the identity of the E9-1-1 network element responsible for serving the geographic area in which the "911" call occurred. If push mode has been selected, then Ap911 automatically pushes the location record to that E9-1-1 network element. If pull mode has been selected, then Ap911 places the
30 location record into a circular table of "911" location records and awaits a query.

The dynamic routing means described above entails the use of a geographically defined database that may be applied to other applications in addition to 911, and is therefore supported by other processes in addition to Ap911. For example, the AP 14 can automatically determine the billing zone from which a wireless call was placed for a

5 Location Sensitive Billing application. In addition, the AP 14 may automatically send an alert when a particular wireless transmitter has entered or exited a prescribed geographic area defined by an application. The use of particular geographic databases, dynamic routing actions, any other location triggered actions are defined in the fields and flags associated with each trigger criteria. The Wireless Location System includes means to

10 easily manage these geographically defined databases using an electronic map that can create polygons encompassing a prescribed geographic area. The Wireless Location System extracts from the electronic map a table of latitude, longitude points contained with the polygon. Each application can use its own set of polygons, and can define a set of actions to be taken when a location record for a triggered wireless transmission is

15 contained within each polygon in the set.

The AP Database Receive Process (ApDbRecvLoc) receives all location records from ApMnDsptch via shared memory, and places the location records into the AP location database. ApDbRecvLoc starts ten threads that each retrieve location records from

20 shared memory, validate each record before inserting the records into the database, and then inserts the records into the correct location record partition in the database. To preserve integrity, location records with any type of error are not written into the location record database but are instead placed into an error file that can be reviewed by the Wireless Location System operator and then manually entered into the database after

25 error resolution. If the location database has failed or has been placed into off-line status, location records are written to a flat file where they can be later processed by ApDbFileRecv.

The AP File Receive Process (ApDbFileRecv) reads flat files containing location records

30 and inserts the records into the location database. Flat files are a safe mechanism used by the AP 14 to completely preserve the integrity of the AP 14 in all cases except a complete failure of the hard disk drives. There are several different types of flat files read

by ApDbFileRecv, including Database Down, Synchronization, Overflow, and Fixed Error. Database Down flat files are written by the ApDbRecvLoc process if the location database is temporarily inaccessible; this file allows the AP 14 to ensure that location records are preserved during the occurrence of this type of problem. Synchronization flat files are written by the ApLocSync process (described below) when transferring location records between pairs of redundant AP systems. Overflow flat files are written by ApMnDsptch when location records are arriving into the AP 14 at a rate faster than ApDbRecvLoc can process and insert the records into the location database. This may occur during very high peak rate periods. The overflow files prevent any records from being lost during peak periods. The Fixed Error flat files contain location records that had errors but have now been fixed, and can now be inserted into the location database.

Because the AP 14 has a critical centralized role in the Wireless Location System, the AP 14 architecture has been designed to be fully redundant. A redundant AP 14 system includes fully redundant hardware platforms, fully redundant RDBMS, redundant disk drives, and redundant networks to each other, the TLP's 12, the NOC's 16, and external applications. The software architecture of the AP 14 has also been designed to support fault tolerant redundancy. The following examples illustrate functionality supported by the redundant AP's. Each TLP 12 sends location records to both the primary and the redundant AP 14 when both AP's are in an online state. Only the primary AP 14 will process incoming tasking requests, and only the primary AP 14 will accept configuration change requests from the NOC 16. The primary AP 14 then synchronizes the redundant AP 14 under careful control. Both the primary and redundant AP's will accept basic startup and shutdown commands from the NOC. Both AP's constantly monitor their own system parameters and application health and monitor the corresponding parameters for the other AP 14, and then decide which AP 14 will be primary and which will be redundant based upon a composite score. This composite score is determined by compiling errors reported by various processes to a shared memory area, and monitoring swap space and disk space. There are several processes dedicated to supporting redundancy.

The AP Location Synchronization Process (ApLocSync) runs on each AP 14 and detects the need to synchronize location records between AP's, and then creates "sync records" that list the location records that need to be transferred from one AP 14 to another AP 14. The location records are then transferred between AP's using a socket connection.

- 5 ApLocSync compares the location record partitions and the location record sequence numbers stored in each location database. Normally, if both the primary and redundant AP 14 are operating properly, synchronization is not needed because both AP's are receiving location records simultaneously from the TLP's 12. However, if one AP 14 fails or is placed in an off-line mode, then synchronization will later be required.
- 10 ApLocSync is notified whenever ApMnDsptch connects to a TLP 12 so it can determine whether synchronization is required.

The AP Tasking Synchronization Process (ApTaskSync) runs on each AP 14 and synchronizes the tasking information between the primary AP 14 and the redundant AP

15 14. ApTaskSync on the primary AP 14 receives tasking information from ApDbSend, and then sends the tasking information to the ApTaskSync process on the redundant AP 14. If the primary AP 14 were to fail before ApTaskSync had completed replicating tasks, then ApTaskSync will perform a complete tasking database synchronization when the failed AP 14 is placed back into an online state.

20

The AP Configuration Synchronization Process (ApConfigSync) runs on each AP 14 and synchronizes the configuration information between the primary AP 14 and the redundant AP 14. ApConfigSync uses a RDBMS replication facility. The configuration information includes all information needed by the SCS's 10, TLP's 12, and AP's 14 for

25 proper operation of the Wireless Location System in a wireless carrier's network.

- In addition to the core functions described above, the AP 14 also supports a large number of processes, functions, and interfaces useful in the operation of the Wireless Location System, as well as useful for various applications that desire location information. While
- 30 the processes, functions, and interfaces described herein are in this section pertaining to the AP 14, the implementation of many of these processes, functions, and interfaces

permeates the entire Wireless Location System and therefore their inventive value should be not read as being limited only to the AP 14.

Roaming

- 5 The AP 14 supports “roaming” between wireless location systems located in different cities or operated by different wireless carriers. If a first wireless transmitter has subscribed to an application on a first Wireless Location System, and therefore has an entry in the Tasking List in the first AP 14 in the first Wireless Location System, then the first wireless transmitter may also subscribe to roaming. Each AP 14 and TLP 12 in each
- 10 Wireless Location System contains a table in which a list of valid “home” subscriber identities is maintained. The list is typically a range, and for example, for current cellular telephones, the range can be determined by the NPA/NXX codes (or area code and exchange) associated with the MIN or MSID of cellular telephones. When a wireless transmitter meeting the “home” criteria makes a transmission, a TLP 12 receives
- 15 demodulated data from one or more SCS’s 10 and checks the trigger information in the Signal of Interest Table . If any trigger criterion is met, the location processing begins on that transmission; otherwise, the transmission is not processed by the Wireless Location System.
- 20 When a first wireless transmitter not meeting the “home” criterion makes a transmission in a second Wireless Location System, the second TLP 12 in the second Wireless Location System checks the Signal of Interest Table for a trigger. One of three actions then occurs: (i) if the transmission meets an already existing criteria in the Signal of Interest Table , the transmitter is located and the location record is forwarded from the
- 25 second AP 14 in the second Wireless Location System to the first AP 14 in the first Wireless Location System; (ii) if the first wireless transmitter has a “roamer” entry in the Signal of Interest Table indicating that the first wireless transmitter has “registered” in the second Wireless Location System but has no trigger criteria, then the transmission is not processed by the second Wireless Location System and the expiration timestamp is
- 30 adjusted as described below; (iii) if the first wireless transmitter has no “roamer” entry and therefore has not “registered”, then the demodulated data is passed from the TLP 12 to the second AP 14.

In the third case above, the second AP 14 uses the identity of the first wireless transmitter to identify the first AP 14 in the first Wireless Location System as the “home” Wireless Location System of the first wireless transmitter. The second AP 14 in the second Wireless Location System sends a query to the first AP 14 in the first Wireless Location System to determine whether the first wireless transmitter has subscribed to any location application and therefore has any trigger criteria in the Tasking List of the first AP 14. If a trigger is present in the first AP 14, the trigger criteria, along with any associated fields and flags, is sent from the first AP 14 to the second AP 14 and entered in the Tasking List and the Signal of Interest Table as a “roamer” entry with trigger criteria. If the first AP 14 responds to the second AP 14 indicating that the first wireless transmitter has no trigger criteria, then the second AP 14 “registers” the first wireless transmitter in the Tasking List and the Signal of Interest Table as a “roamer” with no trigger criteria. Thus both current and future transmissions from the first wireless transmitter can be positively identified by the TLP 12 in the second Wireless Location System as being registered without trigger criteria, and the second AP 14 is not required to make additional queries to the first AP 14.

When the second AP 14 registers the first wireless transmitter with a roamer entry in the Tasking List and the Signal of Interest Table with or without trigger criteria, the roamer entry is assigned an expiration timestamp. The expiration timestamp is set to the current time plus a predetermined first interval. Every time the first wireless transmitter makes a transmission, the expiration timestamp of the roamer entry in the Tasking List and the Signal of Interest Table is adjusted to the current time of the most recent transmission plus the predetermined first interval. If the first wireless transmitter makes no further transmissions prior to the expiration timestamp of its roamer entry, then the roamer entry is automatically deleted. If, subsequent to the deletion, the first wireless transmitter makes another transmission, then the process of registering occurs again.

The first AP 14 and second AP 14 maintain communications over a wide area network. The network may be based upon TCP/IP or upon a protocol similar to the most recent version of IS-41. Each AP 14 in communications with other AP’s in other wireless

location systems maintains a table that provides the identity of each AP 14 and Wireless Location System corresponding to each valid range of identities of wireless transmitters.

Multiple Pass Location Records

- 5 Certain applications may require a very fast estimate of the general location of a wireless transmitter, followed by a more accurate estimate of the location that can be sent subsequently. This can be valuable, for example, for E9-1-1 systems that handle wireless calls and must make a call routing decision very quickly, but can wait a little longer for a more exact location to be displayed upon the E9-1-1 call-taker's electronic map terminal.
- 10 The Wireless Location System supports these applications with an inventive multiple pass location processing mode, described later. The AP 14 supports this mode with multiple pass location records. For certain entries, the Tasking List in the AP 14 contains a flag indicating the maximum time limit before which a particular application must receive a rough estimate of location, and a second maximum time limit in which a
- 15 particular application must receive a final location estimate. For these certain applications, the AP 14 includes a flag in the location record indicating the status of the location estimate contained in the record, which may, for example, be set to first pass estimate (i.e. rough) or final pass estimate. The Wireless Location System will generally determine the best location estimate within the time limit set by the application, that is
- 20 the Wireless Location System will process the most amount of RF data that can be supported in the time limit. Given that any particular wireless transmission can trigger a location record for one or more applications, the Wireless Location System supports multiple modes simultaneously. For example, a wireless transmitter with a particular MIN can dial "911". This may trigger a two-pass location record for the E9-1-1
- 25 application, but a single pass location record for a fleet management application that is monitoring that particular MIN. This can be extended to any number of applications.

Multiple Demodulation and Triggers

- 30 In wireless communications systems in urban or dense suburban areas, frequencies or channels can be re-used several times within relatively close distances. Since the Wireless Location System is capable of independently detecting and demodulating wireless transmissions without the aid of the wireless communications

system, a single wireless transmission can frequently be detected and successfully demodulated at multiple SCS's 10 within the Wireless Location System. This can happen both intentionally and unintentionally. An unintentional occurrence is caused by a close frequency re-use, such that a particular wireless transmission can be received above a predetermined threshold at more than one SCS 10, when each SCS 10 believes it is monitoring only transmissions that occur only within the cell site collocated with the SCS 10. An intentional occurrence is caused by programming more than one SCS 10 to detect and demodulate transmissions that occur at a particular cell site and on a particular frequency. As described earlier, this is generally used with adjacent or nearby SCS's 10 to provide system demodulation redundancy to further increase the probability that any particular wireless transmission is successful detected and demodulated.

Either type of event could potentially lead to multiple triggers within the Wireless Location System, causing location processing to be initiated several times for the same transmission. This causes an excess and inefficient use of processing and communications resources. Therefore, the Wireless Location System includes means to detect when the same transmission has been detected and demodulated more than once, and to select the best demodulating SCS 10 as the starting point for location processing. When the Wireless Location System detects and successfully demodulates the same transmission multiple times at multiple SCS/antennas, the Wireless Location System uses the following criteria to select the one demodulating SCS/antenna to use to continue the process of determining whether to trigger and possibly initiate location processing (again, these criteria may be weighted in determining the final decision): (i) an SCS/antenna collocated at the cell site to which a particular frequency has been assigned is preferred over another SCS/antenna, but this preference may be adjusted if there is no operating and on-line SCS/antenna collocated at the cell site to which the particular frequency has been assigned, (ii) SCS/antennas with higher average SNR are preferred over those with lower average SNR, and (iii) SCS/antennas with fewer bit errors in demodulating the transmission are preferred over those with higher bit errors. The weighting applied to each of these preferences may be adjusted by the operator of the Wireless Location System to suit the particular design of each system.

Interface to Wireless Communications System

The Wireless Location System contains means to communicate over an interface to a wireless communications system, such as a mobile switching center (MSC) or mobile positioning controller (MPC). This interface may be based, for example, on a standard secure protocol such as the most recent version of the IS-41 or TCP/IP protocols. The formats, fields, and authentication aspects of these protocols are well known. The Wireless Location System supports a variety of command / response and informational messages over this interface that are designed to aid in the successful detection, demodulation, and triggering of wireless transmissions, as well as providing means to pass location records to the wireless communications system. In particular, this interface provides means for the Wireless Location System to obtain information about which wireless transmitters have been assigned to particular voice channel parameters at particular cell sites. Example messages supported by the Wireless Location System over this interface to the wireless communications system include the following:

Query on MIN / MDN / MSID / IMSI / TMSI Mapping – Certain types of wireless transmitters will transmit their identity in a familiar form that can be dialed over the telephone network. Other types of wireless transmitters transmit an identity that cannot be dialed, but which is translated into a number that can be dialed using a table inside of the wireless communications system. The transmitted identity is permanent in most cases, but can also be temporary. Users of location applications connected to the AP 14 typically prefer to place triggers onto the Tasking List using identities that can be dialed. Identities that can be dialed are typically known as Mobile Directory Numbers (MDN). The other types of identities for which translation may be required includes Mobile Identity Number (MIN), Mobile Subscriber Identity (MSID), International Mobile Subscriber Identity (IMSI), and Temporary Mobile Subscriber Identity (TMSI). If the wireless communications system has enabled the use of encryption for any of the data fields in the messages transmitted by wireless transmitters, the Wireless Location System may also query for encryption information along with the identity information. The Wireless Location System includes means to query the wireless communications system for the alternate identities for a trigger identity that has been placed onto the Tasking List

by a location application, or to query the wireless communications system for alternate identities for an identity that has been demodulated by an SCS 10. Other events can also trigger this type of query. For this type of query, typically the Wireless Location System initiates the command, and the wireless communications system responds.

Query / Command Change on Voice RF Channel Assignment – Many wireless transmissions on voice channels do not contain identity information. Therefore, when the Wireless Location System is triggered to perform location processing on a voice channel transmission, the Wireless Location System queries the wireless communication system to obtain the current voice channel assignment information for the particular transmitter for which the Wireless Location System has been triggered. For an AMPS transmission, for example, the Wireless Location System preferably requires the cell site, sector, and RF channel number currently in use by the wireless transmitter. For a TDMA transmission, for example, the Wireless Location System preferably requires the cell site, sector, RF channel number, and timeslot currently in use by the wireless transmitter. Other information elements that may be needed include long code mask and encryption keys. In general, the Wireless Location System will initiate the command, and the wireless communications system will respond. However, the Wireless Location System will also accept a trigger command from the wireless communications system that contains the information detailed herein.

The timing on this command / response message set is very critical since voice channel handoffs can occur quite frequently in wireless communications systems. That is, the Wireless Location System will locate any wireless transmitter that is transmitting on a particular channel – therefore the Wireless Location System and the wireless communications system must jointly be certain that the identity of the wireless transmitter and the voice channel assignment information are in perfect synchronization. The Wireless Location System uses several means to achieve this objective. The Wireless Location System may, for example, query the voice channel assignment information for a particular wireless transmitter, receive the necessary RF

data, then again query the voice channel assignment information for that same wireless transmitter, and then verify that the status of the wireless transmitter did not change during the time in which the RF data was being collected by the Wireless Location System. Location processing is not required to complete before the second query, since it is only important to verify that the correct RF data was received. The Wireless Location System may also, for example, as part of the first query command the wireless communications system to prevent a handoff from occurring for the particular wireless transmitter during the time period in which the Wireless Location System is receiving the RF data. Then, subsequent to collecting the RF data, the Wireless Location System will again query the voice channel assignment information for that same wireless transmitter, command the wireless communications system to again permit handoffs for the wireless transmitter and then verify that the status of the wireless transmitter did not change during the time in which the RF data was being collected by the Wireless Location System.

For various reasons, either the Wireless Location System or the wireless communications system may prefer that the wireless transmitter be assigned to another voice RF channel prior to performing location processing. Therefore, as part of the command / response sequence, the wireless communications system may instruct the Wireless Location System to temporarily suspend location processing until the wireless communications system has completed a handoff sequence with the wireless transmitter, and the wireless communications system has notified the Wireless Location System that RF data can be received and the voice RF channel upon which the data can be received. Alternatively, the Wireless Location System may determine that the particular voice RF channel which a particular wireless transmitter is currently using is unsuitable for obtaining an acceptable location estimate, and request that the wireless communications system command the wireless transmitter to handoff. Alternatively, the Wireless Location System may request that the wireless communications system command the wireless transmitter to handoff to a series of voice RF channels in sequence in order to perform a series of location estimates, whereby the Wireless Location System can improve upon the accuracy of

the location estimate through the series of handoffs. This method is further described below.

5 The Wireless Location System can also use this command / response message set to query the wireless communications system about the identity of a wireless transmitter that had been using a particular voice channel (and timeslot, etc.) at a particular cell site at a particular time. This enables the Wireless Location System to first perform location processing on transmissions without knowing the identities, and then to later determine the identity of the wireless transmitters making the transmissions and
10 append this information to the location record. This particular inventive feature enables the use of automatic sequential location of voice channel transmissions.

Receive Triggers – The Wireless Location System can receive triggers from the wireless communications system to perform location processing on a voice channel
15 transmission without knowing the identity of the wireless transmitter. This message set bypasses the Tasking List, and does not use the triggering mechanisms within the Wireless Location System. Rather, the wireless communications system alone determines which wireless transmissions to locate, and then sends a command to the Wireless Location System to collect RF data from a particular voice channel at a
20 particular cell site and to perform location processing. The Wireless Location System responds with a confirmation containing a timestamp when the RF data was collected. The Wireless Location System also responds with an appropriate format location record when location processing has completed. Based upon the time of the command to Wireless Location System and the response with the RF data collection
25 timestamp, the wireless communications system determines whether the wireless transmitter status changed subsequent to the command and whether there is a good probability of successful RF data collection.

30 Make Transmit – The Wireless Location System can command the wireless communications system to force a particular wireless transmitter to make a transmission at a particular time, or within a prescribed range of times. The wireless communications system responds with a confirmation and a time or time range in

which to expect the transmission. The types of transmissions that the Wireless Location System can force include, for example, audit responses and page responses. Using this message set, the Wireless Location System can also command the wireless communications system to force the wireless transmitter to transmit using a higher power level setting. In many cases, wireless transmitters will attempt to use the lowest power level settings when transmitting in order to conserve battery life. In order to improve the accuracy of the location estimate, the Wireless Location System may prefer that the wireless transmitter use a higher power level setting. The wireless communications system will respond to the Wireless Location System with a confirmation that the higher power level setting will be used and a time or time range in which to expect the transmission.

Delay Wireless Communications System Response to Mobile Access – Some air interface protocols, such as CDMA, use a mechanism in which the wireless transmitter initiates transmissions on a channel, such as an Access Channel, for example, at the lowest or a very low power level setting, and then enters a sequence of steps in which (i) the wireless transmitter makes an access transmission; (ii) the wireless transmitter waits for a response from the wireless communications system; (iii) if no response is received by the wireless transmitter from the wireless communications system within a predetermined time, the wireless transmitter increases its power level setting by a predetermined amount, and then returns to step (i); (iv) if a response is received by the wireless transmitter from the wireless communications system within a predetermined time, the wireless transmitter then enters a normal message exchange. This mechanism is useful to ensure that the wireless transmitter uses only the lowest useful power level setting for transmitting and does not further waste energy or battery life. It is possible, however, that the lowest power level setting at which the wireless transmitter can successfully communicate with the wireless communications system is not sufficient to obtain an acceptable location estimate. Therefore, the Wireless Location System can command the wireless communications system to delay its response to these transmissions by a predetermined time or amount. This delaying action will cause the wireless transmitter to repeat the sequence of steps (i) through (iii) one or more times than

- normal with the result that one or more of the access transmissions will be at a higher power level than normal. The higher power level may preferably enable the Wireless Location System to determine a more accurate location estimate. The Wireless Location System may command this type of delaying action for either a particular
- 5 wireless transmitter, for a particular type of wireless transmission (for example, for all '911' calls), for wireless transmitters that are at a specified range from the base station to which the transmitter is attempting to communicate, or for all wireless transmitters in a particular area.
- 10 Send Confirmation to Wireless Transmitter – The Wireless Location System does not include means within itself to notify the wireless transmitter of an action because the Wireless Location System cannot transmit; as described earlier the Wireless Location System can only receive transmissions. Therefore, if the Wireless Location System desires to send, for example, a confirmation tone upon the completion of a certain
- 15 action, the Wireless Location System commands the wireless communications system to transmit a particular message. The message may include, for example, an audible confirmation tone, spoken message, or synthesized message to the wireless transmitter, or a text message sent via a short messaging service or a page. The Wireless Location System receives confirmation from the wireless communications
- 20 system that the message has been accepted and sent to the wireless transmitter. This command / response message set is important in enabling the Wireless Location System to support certain end-user application functions such as Prohibit Location Processing.
- 25 Report Location Records – The Wireless Location System automatically reports location records to the wireless communications system for those wireless transmitters tasked to report to the wireless communications system, as well as for those transmissions that the wireless communications system initiated triggers. The Wireless Location System also reports on any historical location record queried by
- 30 the wireless communications system and which the wireless communications system is authorized to receive.

Monitor Internal Wireless Communications System Interfaces, State Table

In addition to this above interface between the Wireless Location System and the wireless communications system, the Wireless Location System also includes means to monitor existing interfaces within the wireless communications system for the purpose of intercepting messages important to the Wireless Location System for identifying wireless transmitters and the RF channels in use by these transmitters. These interfaces may include, for example, the "A interface" and "Abis interface" used in wireless communications systems employing the GSM air interface protocol. (This aspect of the present invention is described in greater detail below in the section titled "Monitoring of Call Information".) These interfaces are well known and published in various standards. By monitoring the bi-directional messages on these interfaces between base stations (BTS), base station controllers (BSC), and mobile switching centers (MSC), and other points, the Wireless Location System can obtain the same information about the assignment of wireless transmitters to specific channels as the wireless communications system itself knows. The Wireless Location System includes means to monitor these interfaces at various points. For example, the SCS 10 may monitor a BTS to BSC interface. Alternately, a TLP 12 or AP 14 may also monitor a BSC where a number of BTS to BSC interfaces have been concentrated. The interfaces internal to the wireless communications system are not encrypted and the layered protocols are known to those familiar with the art. The advantage to the Wireless Location System to monitoring these interfaces is that the Wireless Location System may not be required to independently detect and demodulate control channel messages from wireless transmitters. In addition, the Wireless Location System may obtain all necessary voice channel assignment information from these interfaces.

25

Using these means for a control channel transmission, the SCS 10 receives the transmissions as described earlier and records the control channel RF data into memory without performing detection and demodulation. Separately, the Wireless Location System monitors the messages occurring over prescribed interfaces within the wireless communications system, and causes a trigger in the Wireless Location System when the Wireless Location System discovers a message containing a trigger event. Initiated by the trigger event, the Wireless Location System determines the approximately time at

30

which the wireless transmission occurred, and commands a first SCS 10 and a second SCS 10B to each search its memory for the start of transmission. This first SCS 10A chosen is an SCS that is either collocated with the base station to which the wireless transmitter had communicated, or an SCS which is adjacent to the base station to which the wireless transmitter had communicated. That is, the first SCS 10A is an SCS which would have been assigned the control channel as a primary channel. If the first SCS 10A successfully determines and reports the start of the transmission, then location processing proceeds normally, using the means described below. If the first SCS 10A cannot successfully determine the start of transmission, then the second SCS 10B reports the start of transmission, and then location processing proceeds normally.

The Wireless Location System also uses these means for voice channel transmissions. For all triggers contained in the Tasking List, the Wireless Location System monitors the prescribed interfaces for messages pertaining to those triggers. The messages of interest include, for example, voice channel assignment messages, handoff messages, frequency hopping messages, power up / power down messages, directed re-try messages, termination messages, and other similar action and status messages. The Wireless Location System continuously maintains a copy of the state and status of these wireless transmitters in a State Table in the AP 14. Each time that the Wireless Location System detects a message pertaining to one of the entries in the Tasking List, the Wireless Location System updates its own State Table. Thereafter, the Wireless Location System may trigger to perform location processing, such as on a regular time interval, and access the State Table to determine precisely which cell site, sector, RF channel, and timeslot is presently being used by the wireless transmitter. The example contained herein described the means by which the Wireless Location System interfaces to a GSM based wireless communications system. The Wireless Location System also supports similar functions with systems based upon other air interfaces.

For certain air interfaces, such as CDMA, the Wireless Location System also keeps certain identity information obtained from Access bursts in the control channel in the State Table; this information is later used for decoding the masks used for voice channels. For example, the CDMA air interface protocol uses the Electronic Serial

Number (ESN) of a wireless transmitter to, in part, determine the long code mask used in the coding of voice channel transmissions. The Wireless Location System maintains this information in the State Table for entries in the Tasking List because many wireless transmitters may transmit the information only once; for example, many CDMA mobiles will only transmit their ESN during the first Access burst after the wireless transmitter become active in a geographic area. This ability to independently determine the long code mask is very useful in cases where an interface between the Wireless Location System and the wireless communications system is not operative and/or the Wireless Location System is not able to monitor one of the interfaces internal to the wireless communications system. The operator of the Wireless Location System may optionally set the Wireless Location System to maintain the identity information for all wireless transmitters. In addition to the above reasons, the Wireless Location System can provide the voice channel tracking for all wireless transmitters that trigger location processing by calling "911". As described earlier, the Wireless Location System uses dynamic tasking to provide location to a wireless transmitter for a prescribed time after dialing "911", for example. By maintaining the identity information for all wireless transmitters in the State Table, the Wireless Location System is able to provide voice channel tracking for all transmitters in the event of a prescribed trigger event, and not just those with prior entries in the Tasking List.

20

Applications Interface

Using the AP 14, the Wireless Location System supports a variety of standards based interfaces to end-user and carrier location applications using secure protocols such as TCP/IP, X.25, SS-7, and IS-41. Each interface between the AP 14 and an external application is a secure and authenticated connection that permits the AP 14 to positively verify the identity of the application that is connected to the AP 14. This is necessary because each connected application is granted only limited access to location records on a real-time and/or historical basis. In addition, the AP 14 supports additional command / response, real-time, and post-processing functions that are further detailed below. Access to these additional functions also requires authentication. The AP 14 maintains a user list and the authentication means associated with each user. No application can gain access to location records or functions for which the application does not have proper

authentication or access rights. In addition, the AP 14 supports full logging of all actions taken by each application in the event that problems arise or a later investigation into actions is required. For each command or function in the list below, the AP 14 preferably supports a protocol in which each action or the result of each is confirmed, as
5 appropriate.

Edit Tasking List – This command permits external applications to add, remove, or edit entries in the Tasking List, including any fields and flags associated with each entry.

This command can be supported on a single entry basis, or a batch entry basis where a
10 list of entries is included in a single command. The latter is useful, for example, in a bulk application such as location sensitive billing whereby larger volumes of wireless transmitters are being supported by the external application, and it is desired to minimize protocol overhead. This command can add or delete applications for a particular entry in the Tasking List, however, this command cannot delete an entry entirely if the entry also
15 contains other applications not associated with or authorized by the application issuing the command.

Set Location Interval – The Wireless Location System can be set to perform location processing at any interval for a particular wireless transmitter, on either control or voice
20 channels. For example, certain applications may require the location of a wireless transmitter every few seconds when the transmitter is engaged on a voice channel. When the wireless transmitter make an initial transmission, the Wireless Location System initially triggers using a standard entry in the Tasking List. If one of the fields or flags in this entry specifies updated location on a set interval, then the Wireless Location System
25 creates a dynamic task in the Tasking List that is triggered by a timer instead of an identity or other transmitted criteria. Each time the timer expires, which can range from 1 second to several hours, the Wireless Location System will automatically trigger to locate the wireless transmitter. The Wireless Location System uses its interface to the wireless communications system to query status of the wireless transmitter, including
30 voice call parameters as described earlier. If the wireless transmitter is engaged on a voice channel, then the Wireless Location System performs location processing. If the wireless transmitter is not engaged in any existing transmissions, the Wireless Location

System will command the wireless communications system to make the wireless transmitter immediately transmit. When the dynamic task is set, the Wireless Location System also sets an expiration time at which the dynamic task ceases.

- 5 End-User Addition / Deletion – This command can be executed by an end-user of a wireless transmitter to place the identity of the wireless transmitter onto the Tasking List with location processing enabled, to remove the identity of the wireless transmitter from the Tasking List and therefore eliminate identity as a trigger, or to place the identity of the wireless transmitter onto the Tasking List with location processing disabled. When
- 10 location processing has been disabled by the end-user, known as Prohibit Location Processing then no location processing will be performed for the wireless transmitter. The operator of the Wireless Location System can optionally select one of several actions by the Wireless Location System in response to a Prohibit Location Processing command by the end user: (i) the disabling action can override all other triggers in the
- 15 Tasking List, including a trigger due to an emergency call such as “911”, (ii) the disabling action can override any other trigger in the Tasking List, except a trigger due to an emergency call such as “911”, (iii) the disabling action can be overridden by other select triggers in the Tasking List. In the first case, the end-user is granted complete control over the privacy of the transmissions by the wireless transmitter, as no location
- 20 processing will be performed on that transmitter for any reason. In the second case, the end-user may still receive the benefits of location during an emergency, but at no other times. In an example of the third case, an employer who is the real owner of a particular wireless transmitter can override an end-user action by an employee who is using the wireless transmitter as part of the job but who may not desire to be located. The Wireless
- 25 Location System may query the wireless communications system, as described above, to obtain the mapping of the identity contained in the wireless transmission to other identities.

- The additions and deletions by the end-user are effected by dialed sequences of
- 30 characters and digits and pressing the “SEND” or equivalent button on the wireless transmitter. These sequences may be optionally chosen and made known by the operator of the Wireless Location System. For example, one sequence may be “*55 SEND” to

disable location processing. Other sequences are also possible. When the end-user can dialed this prescribed sequence, the wireless transmitter will transmit the sequence over one of the prescribed control channels of the wireless communications system. Since the Wireless Location System independently detects and demodulates all reverse control

5 channel transmissions, the Wireless Location System can independently interpret the prescribed dialed sequence and make the appropriate feature updates to the Tasking List, as described above. When the Wireless Location System has completed the update to the Tasking List, the Wireless Location System commands the wireless communications system to send a confirmation to the end-user. As described earlier, this may take the

10 form of an audible tone, recorded or synthesized voice, or a text message. This command is executed over the interface between the Wireless Location System and the wireless communications system.

Command Transmit – This command allows external applications to cause the Wireless

15 Location System to send a command to the wireless communications system to make a particular wireless transmitter, or group of wireless transmitters, transmit. This command may contain a flag or field that the wireless transmitter(s) should transmit immediately or at a prescribed time. This command has the effort of locating the wireless transmitter(s) upon command, since the transmissions will be detected, demodulated, and triggered,

20 causing location processing and the generation of a location record. This is useful in eliminating or reducing any delay in determining location such as waiting for the next registration time period for the wireless transmitter or waiting for an independent transmission to occur.

25 External Database Query and Update – The Wireless Location System includes means to access an external database, to query the said external database using the identity of the wireless transmitter or other parameters contained in the transmission or the trigger criteria, and to merge the data obtained from the external database with the data generated by the Wireless Location System to create a new enhanced location record.

30 The enhanced location record may then be forwarded to requesting applications. The external database may contain, for example, data elements such as customer information, medical information, subscribed features, application related information, customer

account information, contact information, or sets of prescribed actions to take upon a location trigger event. The Wireless Location System may also cause updates to the external database, for example, to increment or decrement a billing counter associated with the provision of location services, or to update the external database with the latest
5 location record associated with the particular wireless transmitter. The Wireless Location System contains means to performed the actions described herein on more than one external database. The list and sequence of external databases to access and the subsequent actions to take are contained in one of the fields contained in the trigger criteria in the Tasking List.

10

Random Anonymous Location Processing – The Wireless Location System includes means to perform large scale random anonymous location processing. This function is valuable to certain types of applications that require the gathering of a large volume of data about a population of wireless transmitters without consideration to the specific
15 identities of the individual transmitters. Applications of this type include: RF Optimization, which enables wireless carriers to measure the performance of the wireless communications system by simultaneously determining location and other parameters of a transmission; Traffic Management, which enables government agencies and commercial concerns to monitor the flow of traffic on various highways using
20 statistically significant samples of wireless transmitters travelling in vehicles; and Local Traffic Estimation, which enables commercial enterprises to estimate the flow of traffic around a particular area which may help determine the viability of particular businesses.

Applications requesting random anonymous location processing optionally receive
25 location records from two sources: (i) a copy of location records generated for other applications, and (ii) location records which have been triggered randomly by the Wireless Location System without regard to any specific criteria. All of the location records generated from either source are forwarded with all of the identity and trigger criteria information removed from the location records; however, the requesting
30 application(s) can determine whether the record was generated from the fully random process or is a copy from another trigger criteria. The random location records are generated by a low priority task within the Wireless Location System that performs

location processing on randomly selected transmissions whenever processing and communications resources are available and would otherwise be unused at a particular instant in time. The requesting application(s) can specify whether the random location processing is performed over the entire coverage area of a Wireless Location System, over specific geographic areas such as along prescribed highways, or by the coverage areas of specific cell sites. Thus, the requesting application(s) can direct the resources of the Wireless Location System to those area of greatest interest to each application. Depending on the randomness desired by the application(s), the Wireless Location System can adjust preferences for randomly selecting certain types of transmissions, for example, registration messages, origination messages, page response messages, or voice channel transmissions.

Anonymous Tracking of a Geographic Group – The Wireless Location System includes means to trigger location processing on a repetitive basis for anonymous groups of wireless transmitters within a prescribed geographic area. For example, a particular location application may desire to monitor the travel route of a wireless transmitter over a prescribed period of time, but without the Wireless Location System disclosing the particular identity of the wireless transmitter. The period of time may be many hours, days, or weeks. Using the means, the Wireless Location System: randomly selects a wireless transmitter that initiates a transmission in the geographic area of interest to the application; performs location processing on the transmission of interest; irreversibly translates and encrypts the identity of the wireless transmitter into a new coded identifier; creates a location record using only the new coded identifier as an identifying means; forwards the location record to the requesting location application(s); and creates a dynamic task in the Tasking List for the wireless transmitter, wherein the dynamic task has an associated expiration time. Subsequently, whenever the prescribed wireless transmitter initiates transmission, the Wireless Location System may trigger using the dynamic task, perform location processing on the transmission of interest, irreversibly translate and encrypt the identity of the wireless transmitter into the new coded identifier using the same means as prior such that the coded identifier is the same, create a location record using the coded identifier, and forward the location record to the requesting location application(s). The means described herein can be combined with other

functions of the Wireless Location System to perform this type of monitoring use either control or voice channel transmissions. Further, the means described herein completely preserve the private identity of the wireless transmitter, yet enables another class of applications that can monitor the travel patterns of wireless transmitters. This class of applications can be of great value in determining the planning and design of new roads, alternate route planning, or the construction of commercial and retail space.

Location Record Grouping, Sorting, and Labeling – The Wireless Location System include means to post-process the location records for certain requesting applications to group, sort, or label the location records. For each interface supported by the Wireless Location System, the Wireless Location System stores a profile of the types of data for which the application is both authorized and requesting, and the types of filters or post-processing actions desired by the application. Many applications, such as the examples contained herein, do not require individual location records or the specific identities of individual transmitters. For example, an RF optimization application derives more value from a large data set of location records for a particular cell site or channel than it can from any individual location record. For another example, a traffic monitoring application requires only location records from transmitters that are on prescribed roads or highways, and additionally requires that these records be grouped by section of road or highway and by direction of travel. Other applications may request that the Wireless Location System forward location records that have been formatted to enhance visual display appeal by, for example, adjusting the location estimate of the transmitter so that the transmitter's location appears on an electronic map directly on a drawn road segment rather than adjacent to the road segment. Therefore, the Wireless Location System preferably "snaps" the location estimate to the nearest drawn road segment.

The Wireless Location System can filter and report location records to an application for wireless transmitters communicating only on a particular cell site, sector, RF channel, or group of RF channels. Before forwarding the record to the requesting application, the Wireless Location System first verifies that the appropriate fields in the record satisfy the requirements. Records not matching the requirements are not forwarded, and records matching the requirements are forwarded. Some filters are geographic and must be

calculated by the Wireless Location System. For example, the Wireless Location System can process a location record to determine the closest road segment and direction of travel of the wireless transmitter on the road segment. The Wireless Location System can then forward only records to the application that are determined to be on a particular road segment, and can further enhance the location record by adding a field containing the determined road segment. In order to determine the closest road segment, the Wireless Location System is provided with a database of road segments of interest by the requesting application. This database is stored in a table where each road segment is stored with a latitude and longitude coordinate defining the end point of each segment.

Each road segment can be modeled as a straight or curved line, and can be modeled to support one or two directions of travel. Then for each location record determined by the Wireless Location System, the Wireless Location System compares the latitude and longitude in the location record to each road segment stored in the database, and determines the shortest distance from a modeled line connecting the end points of the segment to the latitude and longitude of the location record. The shortest distance is a calculated imaginary line orthogonal to the line connecting the two end points of the stored road segment. When the closest road segment has been determined, the Wireless Location System can further determine the direction of travel on the road segment by comparing the direction of travel of the wireless transmitter reported by the location processing to the orientation of the road segment. The direction that produces the smallest error with respect to the orientation of the road segments is then reported by the Wireless Location System.

Network Operations Console (NOC) 16

The NOC 16 is a network management system that permits operators of the Wireless Location System easy access to the programming parameters of the Wireless Location System. For example, in some cities, the Wireless Location System may contain many hundreds or even thousands of SCS's 10. The NOC is the most effective way to manage a large Wireless Location System, using graphical user interface capabilities. The NOC will also receive real time alerts if certain functions within the Wireless Location System are not operating properly. These real time alerts can be used by the operator to take corrective action quickly and prevent a degradation of location

service. Experience with trials of the Wireless Location System show that the ability of the system to maintain good location accuracy over time is directly related to the operator's ability to keep the system operating within its predetermined parameters.

5 Location Processing

The Wireless Location System is capable of performing location processing using two different methods known as central based processing and station based processing. Both techniques were first disclosed in Patent Number 5,327,144, and are further enhanced in this specification. Location processing depends in part on the ability to

10 accurately determine certain phase characteristics of the signal as received at multiple antennas and at multiple SCS's 10. Therefore, it is an object of the Wireless Location System to identify and remove sources of phase error that impede the ability of the location processing to determine the phase characteristics of the received signal. One source of phase error is inside of the wireless transmitter itself, namely the oscillator

15 (typically a crystal oscillator) and the phase lock loops that allow the phone to tune to specific channels for transmitting. Lower cost crystal oscillators will generally have higher phase noise. Some air interface specifications, such as IS-136 and IS-95A, have specifications covering the phase noise with which a wireless telephone can transmit. Other air interface specifications, such as IS-553A, do not closely specify phase noise. It

20 is therefore an object of the present invention to automatically reduce and/or eliminate a wireless transmitter's phase noise as a source of phase error in location processing, in part by automatically selecting the use of central based processing or station based processing. The automatic selection will also consider the efficiency with which the communications link between the SCS 10 and the TLP 12 is used, and the availability of

25 DSP resources at each of the SCS 10 and TLP 12.

When using central based processing, the TDOA and FDOA determination and the multipath processing are performed in the TLP 12 along with the position and speed determination. This method is preferred when the wireless transmitter has a phase noise

30 that is above a predetermined threshold. In these cases, central based processing is most effective in reducing or eliminating the phase noise of the wireless transmitter as a source of phase error because the TDOA estimate is performed using a digital

representation of the actual RF transmission from two antennas, which may be at the same SCS 10 or different SCS's 10. In this method, those skilled in the art will recognize that the phase noise of the transmitter is a common mode noise in the TDOA processing, and therefore is self-canceling in the TDOA determination process. This method works
5 best, for example, with many very low cost AMPS cellular telephones that have a high phase noise. The basic steps in central based processing include the steps recited below and represented in the flowchart of Figure 6:

a wireless transmitter initiates a transmission on either a control channel or a voice
10 channel (step S50);
the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S51);
the transmission is converted into a digital format in the receiver connected to each SCS/antenna (step S52);
15 the digital data is stored in a memory in the receivers in each SCS 10 (step S53);
the transmission is demodulated (step S54);
the Wireless Location System determines whether to begin location processing for the transmission (step S55);
if triggered, the TLP 12 requests copies of the digital data from the memory in
20 receivers at multiple SCS's 10 (step S56);
digital data is sent from multiple SCS's 10 to a selected TLP 12 (step S57);
the TLP 12 performs TDOA, FDOA, and multipath mitigation on the digital data from pairs of antennas (step S58);
the TLP 12 performs position and speed determination using the TDOA data, and then
25 creates a location record and forwards the location record to the AP 14 (step S59).

The Wireless Location System uses a variable number of bits to represent the transmission when sending digital data from the SCS's 10 to the TLP 12. As discussed earlier, the SCS receiver digitizes wireless transmissions with a high resolution, or a high
30 number of bits per digital sample in order to achieve a sufficient dynamic range. This is especially required when using wideband digital receivers, which may be simultaneously receiving signals near to the SCS 10A and far from the SCS 10B. For example, up to 14

bits may be required to represent a dynamic range of 84 dB. Location processing does not always require the high resolution per digital sample, however. Frequently, locations of sufficient accuracy are achievable by the Wireless Location System using a fewer number of bits per digital sample. Therefore, to minimize the implementation cost of the

5 Wireless Location System by conserving bandwidth on the communication links between each SCS 10 and TLP 12, the Wireless Location System determines the fewest number of bits required to digitally represent a transmission while still maintaining a desired accuracy level. This determination is based, for example, on the particular air interface protocol used by the wireless transmitter, the SNR of the transmission, the

10 degree to which the transmission has been perturbed by fading and/or multipath, and the current state of the processing and communication queues in each SCS 10. The number of bits sent from the SCS 10 to the TLP 12 are reduced in two ways: the number of bits per sample is minimized, and the shortest length, or fewest segments, of the transmission possible is used for location processing. The TLP 12 can use this minimal RF data to

15 perform location processing and then compare the result with the desired accuracy level. This comparison is performed on the basis of a confidence interval calculation. If the location estimate does not fall within the desired accuracy limits, the TLP 12 will recursively request additional data from selected SCS's 10. The additional data may include an additional number of bits per digital sample and/or may include more

20 segments of the transmission. This process of requesting additional data may continue recursively until the TLP 12 has achieved the prescribed location accuracy.

There are additional details to the basic steps described above. These details are described in prior Patent Numbers 5,327,144 and 5,608,410 in other parts of this

25 specification. One enhancement to the processes described in earlier patents is the selection of a single reference SCS/antenna that is used for each baseline in the location processing. In prior art, baselines were determined using pairs of antenna sites around a ring. In the present Wireless Location System, the single reference SCS/antenna used is generally the highest SNR signal, although other criteria are also used as described

30 below. The use of a high SNR reference aids central based location processing when the other SCS/antennas used in the location processing are very weak, such as at or below the noise floor (i.e. zero or negative signal to noise ratio). When station based location

processing is used, the reference signal is a re-modulated signal, which is intentionally created to have a very high signal to noise ratio, further aiding location processing for very weak signals at other SCS/antennas. The actual selection of the reference SCS/antenna is described below.

5

The Wireless Location System mitigates multipath by first recursively estimating the components of multipath received in addition to the direct path component and then subtracting these components from the received signal. Thus the Wireless Location System models the received signal and compares the model to the actual received signal
10 and attempts to minimize the difference between the two using a weighted least square difference. For each transmitted signal $x(t)$ from a wireless transmitter, the received signal $y(t)$ at each SCS/antenna is a complex combination of signals:

$$y(t) = \sum x(t - \tau_n) a_n e^{j\omega(t - \tau_n)}, \text{ for all } n = 0 \text{ to } N;$$

15

where $x(t)$ is the signal as transmitted by the wireless transmitter;
 a_n and τ_n are the complex amplitude and delays of the multipath components;
 N is the total number of multipath components in the received signal; and
 a_0 and τ_0 are constants for the most direct path component.

20

The operator of the Wireless Location System empirically determines a set of constraints for each component of multipath that applies to the specific environment in which each Wireless Location System is operating. The purpose of the constraints is to limit the amount of processing time that the Wireless Location System spends optimizing the
25 results for each multipath mitigation calculation. For example, the Wireless Location System may be set to determine only four components of multipath: the first component may be assumed to have a time delay in the range τ_{1A} to τ_{1B} ; the second component may be assumed to have a time delay in the range τ_{2A} to τ_{2B} ; the third component may be assumed to have a time delay in the range τ_{3A} to τ_{3B} ; and similar for the fourth
30 component; however the fourth component is a single value that effectively represents a complex combination of many tens of individual (and somewhat diffuse) multipath

components whose time delays exceed the range of the third component. For ease of processing, the Wireless Location System transforms the prior equation into the frequency domain, and then solves for the individual components such that a weighted least squares difference is minimized.

5

When using station based processing, the TDOA and FDOA determination and multipath mitigation are performed in the SCS's 10, while the position and speed determination are typically performed in the TLP 12. The main advantage of station based processing, as described in Patent Number 5,327,144, is reducing the amount of data that is sent on the communication link between each SCS 10 and TLP 12. However, there may be other advantages as well. One new objective of the present invention is increasing the effective signal processing gain during the TDOA processing. As pointed out earlier, central based processing has the advantage of eliminating or reducing phase error caused by the phase noise in the wireless transmitter. However, no previous disclosure has addressed how to eliminate or reduce the same phase noise error when using station based processing. The present invention reduces the phase error and increases the effective signal processing gain using the steps recited below and shown in Figure 6:

a wireless transmitter initiates a transmission on either a control channel or a voice channel (step S60);
the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S61);
the transmission is converted into a digital format in the receiver connected to each antenna (step S62);
the digital data is stored in a memory in the SCS 10 (step S63);
the transmission is demodulated (step S64);
the Wireless Location System determines whether to begin location processing for the transmission (step S65);
if triggered, a first SCS 10A demodulates the transmission and determines an appropriate phase correction interval (step S66);
for each such phase correction interval, the first SCS 10A calculates an appropriate phase correction and amplitude correction, and encodes this phase correction

- parameter and amplitude correction parameter along with the demodulated data (step S67);
- the demodulated data and phase correction and amplitude correction parameters are sent from the first SCS 10A to a TLP 12 (step S68);
- 5 the TLP 12 determines the SCS's 10 and receiving antennas to use in the location processing (step S69);
- the TLP 12 sends the demodulated data and phase correction and amplitude correction parameters to each second SCS 10B that will be used in the location processing (step S70);
- 10 the first SCS 10 and each second SCS 10B creates a first re-modulated signal based upon the demodulated data and the phase correction and amplitude correction parameters (step S71);
- the first SCS 10A and each second SCS 10B performs TDOA, FDOA, and multipath mitigation using the digital data stored in memory in each SCS 10 and the first re-
- 15 modulated signal (step S72);
- the TDOA, FDOA, and multipath mitigation data are sent from the first SCS 10A and each second SCS 10B to the TLP 12 (step S73);
- the TLP 12 performs position and speed determination using the TDOA data (step S74); and
- 20 the TLP 12 creates a location record, and forwards the location record to the AP 14 (step S75).

The advantages of determining phase correction and amplitude correction parameters are most obvious in the location of CDMA wireless transmitters based upon IS-95A. As is

25 well known, the reverse transmissions from an IS-95A transmitter are sent using non-coherent modulation. Most CDMA base stations only integrate over a single bit interval because of the non-coherent modulation. For a CDMA Access Channel, with a bit rate of 4800 bits per second, there are 256 chips sent per bit, which permits an integration gain of 24 dB. Using the technique described above, the TDOA processing in each SCS 10

30 may integrate, for example, over a full 160 millisecond burst (196,608 chips) to produce an integration gain of 53 dB. This additional processing gain enables the present

invention to detect and locate CDMA transmissions using multiple SCS's 10, even if the base stations collocated with the SCS's 10 cannot detect the same CDMA transmission.

For a particular transmission, if either the phase correction parameters or the amplitude
5 correction parameters are calculated to be zero, or are not needed, then these parameters
are not sent in order to conserve on the number of bits transmitted on the
communications link between each SCS 10 and TLP 12. In another embodiment of the
invention, the Wireless Location System may use a fixed phase correction interval for a
particular transmission or for all transmissions of a particular air interface protocol, or
10 for all transmissions made by a particular type of wireless transmitter. This may, for
example, be based upon empirical data gathered over some period of time by the
Wireless Location System showing a reasonable consistency in the phase noise exhibited
by various classes of transmitters. In these cases, the SCS 10 may save the processing
step of determining the appropriate phase correction interval.

15 Those skilled in the art will recognize that there are many ways of measuring the phase
noise of a wireless transmitter. In one embodiment, a pure, noiseless re-modulated copy
of the signal received at the first SCS 10A may be digitally generated by DSP's in the
SCS, then the received signal may be compared against the pure signal over each phase
20 correction interval and the phase difference may be measured directly. In this
embodiment, the phase correction parameter will be calculated as the negative of the
phase difference over that phase correction interval. The number of bits required to
represent the phase correction parameter will vary with the magnitude of the phase
correction parameter, and the number of bits may vary for each phase correction interval.
25 It has been observed that some transmissions, for example, exhibit greater phase noise
early in the transmission, and less phase noise in the middle of and later in the
transmission.

Station based processing is most useful for wireless transmitters that have relatively low
30 phase noise. Although not necessarily required by their respective air interface standards,
wireless telephones that use the TDMA, CDMA, or GSM protocols will typically exhibit
lower phase noise. As the phase noise of a wireless transmitter increases, the length of a

phase correction interval may decrease and/or the number of bits required to represent the phase correction parameters increases. Station based processing is not effective when the number of bits required to represent the demodulated data plus the phase correction and amplitude parameters exceeds a predetermined proportion of the number of bits required to perform central based processing. It is therefore an object of the present invention to automatically determine for each transmission for which a location is desired whether to process the location using central based processing or station based processing. The steps in making this determination are recited below and shown in Figure 7:

- 10 a wireless transmitter initiates a transmission on either a control channel or a voice channel (step S80);
- the transmission is received at a first SCS 10A (step S81);
- the transmission is converted into a digital format in the receiver connected to each
- 15 antenna (step S82);
- the Wireless Location System determines whether to begin location processing for the transmission (step S83);
- if triggered, a first SCS 10A demodulates the transmission and estimates an appropriate phase correction interval and the number of bits required to encode the phase
- 20 correction and amplitude correction parameters (step S84);
- the first SCS 10A then estimates the number of bits required for central based processing;
- based upon the number of bits required for each respective method, the SCS 10 or the TLP 12 determine whether to use central based processing or station based
- 25 processing to perform the location processing for this transmission (step S85).

In another embodiment of the invention, the Wireless Location System may always use central based processing or station based processing for all transmissions of a particular air interface protocol, or for all transmissions made by a particular kind of wireless

30 transmitter. This may, for example, be based upon empirical data gathered over some period of time by the Wireless Location System showing a reasonable consistency in the phase noise exhibited by various classes of transmitters. In these cases, the SCS 10

and/or the TLP 12 may be saved the processing step of determining the appropriate processing method.

A further enhancement of the present invention, used for both central based processing and station based processing, is the use of threshold criteria for including baselines in the final determination of location and velocity of the wireless transmitter. For each baseline, the Wireless Location System calculates a number of parameters that include: the SCS/antenna port used with the reference SCS/antenna in calculating the baseline, the peak, average, and variance in the power of the transmission as received at the SCS/antenna port used in the baseline and over the interval used for location processing, the correlation value from the cross-spectra correlation between the SCS/antenna used in the baseline and the reference SCS/antenna, the delay value for the baseline, the multipath mitigation parameters, the residual values remaining after the multipath mitigation calculations, the contribution of the SCS/antenna to the weighted GDOP in the final location solution, and a measure of the quality of fit of the baseline if included in the final location solution. Each baseline is included in the final location solution is each meets or exceeds the threshold criteria for each of the parameters described herein. A baseline may be excluded from the location solution if it fails to meet one or more of the threshold criteria. Therefore, it is frequently possible that the number of SCS/antennas actually used in the final location solution is less than the total number considered.

Previous Patent Numbers 5,327,144 and 5,608,410 disclosed a method by which the location processing minimized the least square difference (LSD) value of the following equation:

$$\text{LSD} = [Q_{12}(\text{Delay_T}_{12} - \text{Delay_O}_{12})^2 + Q_{13}(\text{Delay_T}_{13} - \text{Delay_O}_{13})^2 + \dots + Q_{xy}(\text{Delay_T}_{xy} - \text{Delay_O}_{xy})^2]$$

In the present implementation, this equation has been rearranged to the following form in order to make the location processing code more efficient:

$$\text{LSD} = \sum (\text{TDOA}_{0i} - \tau_i + \tau_0)^2 w_i^2; \text{ over all } i=1 \text{ to } N-1$$

where N = number of SCS/antennas used in the location processing;

TDOA_{0i} = the TDOA to the i^{th} site from reference site 0;

5 τ_i = the theoretical line of sight propagation time from the wireless transmitter to the i^{th} site;

τ_0 = the theoretical line of sight propagation time from the transmitter to the reference;
and

w_i = the weight, or quality factor, applied to the i^{th} baseline.

10

In the present implementation, the Wireless Location System also uses another alternate form of the equation that can aid in determining location solutions when the reference signal is not very strong or when it is likely that a bias would exist in the location solution using the prior form of the equation:

15

$$\text{LSD}' = \sum (\text{TDOA}_{0i} - \tau_i)^2 w_i^2 - b^2 \sum w_i^2; \text{ over all } i=0 \text{ to } N-1$$

Where N = number of SCS/antennas used in the location processing;

TDOA_{0i} = the TDOA to the i^{th} site from reference site 0;

20 TDOA_{00} = is assumed to be zero;

τ_i = the theoretical line of sight propagation time from the wireless transmitter to the i^{th} site;

b = a bias that is separately calculated for each theoretical point that minimizes LSD' at that theoretical point; and

25 w_i = the weight, or quality factor, applied to the i^{th} baseline.

The LSD' form of the equation offers an easier means of removing a bias in location solutions at the reference site by making w_0 equal to the maximum value of the other weights or basing w_0 on the relative signal strength at the reference site. Note that if w_0 is
30 much larger than the other weights, then b is approximately equal to τ_0 . In general, the weights, or quality factors are based on similar criteria to that discussed above for the

threshold criteria in including baselines. That is, the results of the criteria calculations are used for weights and when the criteria falls below threshold the weight is then set to zero and is effectively not included in the determination of the final location solution.

5 Antenna Selection Process for Location Processing

Previous inventions and disclosures, such as those listed above, have described techniques in which a first, second, or possibly third antenna site, cell site, or base station are required to determine location. Patent number 5,608,410 further discloses a Dynamic Selection Subsystem (DSS) that is responsible for determining which data frames from
10 which antenna site locations will be used to calculate the location of a responsive transmitter. In the DSS, if data frames are received from more than a threshold number of sites, the DSS determines which are candidates for retention or exclusion, and then dynamically organizes data frames for location processing. The DSS prefers to use more than the minimum number of antenna sites so that the solution is over-determined.
15 Additionally, the DSS assures that all transmissions used in the location processing were received from the same transmitter and from the same transmission.

The preferred embodiments of the prior inventions had several limitations, however. First, either only one antenna per antenna site (or cell site) is used, or the data from two
20 or four diversity antennas were first combined at the antenna site (or cell site) prior to transmission to the central site. Additionally, all antenna sites that received the transmission sent data frames to the central site, even if the DSS later discarded the data frames. Thus, some communications bandwidth may have been wasted sending data that was not used.

25

The present inventors have determined that while a minimum of two or three sites are required in order determine location, the actual selection of antennas and SCS's 10 to use in location processing can have a significant effect on the results of the location processing. In addition, it is advantageous to include the means to use more than one
30 antenna at each SCS 10 in the location processing. The reason for using data from multiple antennas at a cell site independently in the location processing is that the signal received at each antenna is uniquely affected by multipath, fading, and other

disturbances. It is well known in the field that when two antennas are separated in distance by more than one wavelength, then each antenna will receive the signal on an independent path. Therefore, there is frequently additional and unique information to be gained about the location of the wireless transmitter by using multiple antennas, and the
5 ability of the Wireless Location System to mitigate multipath is enhanced accordingly.

It is therefore an object of the present invention to provide an improved method for using the signals received from more than one antenna at an SCS 10 in the location processing. It is a further object to provide a method to improve the dynamic process used to select
10 the cooperating antennas and SCS's 10 used in the location processing. The first object is achieved by providing means within the SCS 10 to select and use any segment of data collected from any number of antennas at an SCS in the location processing. As described earlier, each antenna at a cell site is connected to a receiver internal to the SCS 10. Each receiver converts signals received from the antenna into a digital form, and then
15 stores the digitized signals temporarily in a memory in the receiver. The TLP 12 has been provided with means to direct any SCS 10 to retrieve segments of data from the temporary memory of any receiver, and to provide the data for use in location processing. The second object is achieved by providing means within the Wireless Location System to monitor a large number of antennas for reception of the transmission
20 that the Wireless Location System desires to locate, and then selecting a smaller set of antennas for use in location processing based upon a predetermined set of parameters.

One example of this selection process is represented by the flowchart of Figure 8:

- a wireless transmitter initiates a transmission on either a control channel or a voice
25 channel (step S90);
- the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S91);
- the transmission is converted into a digital format in the receiver connected to each antenna (step S92);
- 30 the digital data is stored in a memory in each SCS 10 (step S93);

the transmission is demodulated at at least one SCS 10A and the channel number on which the transmission occurred and the cell site and sector serving the wireless transmitter is determined (step S94);

based upon the serving cell site and sector, one SCS 10A is designated as the 'primary' SCS 10 for processing that transmission (step S95);

the primary SCS 10A determines a timestamp associated with the demodulated data (step S96);

the Wireless Location System determines whether to begin location processing for the transmission (step S97);

if location processing is triggered, the Wireless Location System determines a candidate list of SCS's 10 and antennas to use in the location processing (step S98);

each candidate SCS/antenna measures and reports several parameters in the channel number of the transmission and at the time of the timestamp determined by the primary SCS 10A (step S99);

the Wireless Location System orders the candidate SCS/antennas using specified criteria and selects a reference SCS/antenna and a processing list of SCS/antennas to use in the location processing (step S100); and

the Wireless Location System proceeds with location processing as described earlier, using data from the processing list of SCS/antennas (step S101).

20

Selecting Primary SCS/Antenna

The process for choosing the 'primary' SCS/antenna is critical, because the candidate list of SCS's 10 and antennas 10-1 is determined in part based upon the designation of the primary SCS/antenna. When a wireless transmitter makes a transmission on a particular RF channel, the transmission frequently can propagate many miles before the signal attenuates below a level at which it can be demodulated. Therefore, there are frequently many SCS/antennas capable of demodulating the signal. This especially occurs in urban and suburban areas where the frequency re-use pattern of many wireless communications systems can be quite dense. For example, because of the high usage rate of wireless and the dense cell site spacing, the present inventors have tested wireless communications systems in which the same RF control channel and digital color code were used on cell sites spaced about one mile apart. Because the

- Wireless Location System is independently demodulating these transmissions, the Wireless Location System frequently can demodulate the same transmission at two, three, or more separate SCS/antennas. The Wireless Location System detects that the same transmission has been demodulated multiple times at multiple SCS/antennas when the Wireless Location System receives multiple demodulated data frames sent from different SCS/antennas, each with a number of bit errors below a predetermined bit error threshold, and with the demodulated data matching within an acceptable limit of bit errors, and all occurring within a predetermined interval of time.
- 10 When the Wireless Location System detects demodulated data from multiple SCS/antennas, it examines the following parameters to determine which SCS/antenna may be designated the primary SCS: average SNR over the transmission interval used for location processing, the variance in the SNR over the same interval, correlation of the beginning of the received transmission against a pure pre-cursor (i.e. for AMPS, the dotting and Barker code), the number of bit errors in the demodulated data, and the magnitude and rate of change of the SNR from just before the on-set of the transmission to the on-set of the transmission, as well as other similar parameters. The average SNR is typically determined at each SCS/antenna either over the entire length of the transmission to be used for location processing, or over a shorter interval. The average
- 20 SNR over the shorter interval can be determined by performing a correlation with the dotting sequence and/or Barker code and/or sync word, depending on the particular air interface protocol, and over a short range of time before, during, and after the timestamp reported by each SCS 10. The time range may typically be +/-200 microseconds centered at the timestamp, for example. The Wireless Location System will generally order the
- 25 SCS/antennas using the following criteria, each of which may be weighted (multiplied by an appropriate factor) when combining the criteria to determine the final decision: SCS/antennas with a lower number of bit errors are preferred to SCS/antennas with a higher number of bit errors, average SNR for a given SCS/antenna must be greater than a predetermined threshold to be designated as the primary; SCS/antennas with higher
- 30 average SNR are preferred over those with lower average SNR; SCS/antennas with lower SNR variance are preferred to those with higher SNR variance; and SCS/antennas with a faster SNR rate of change at the on-set of the transmission are preferred to those

with a slower rate of change. The weighting applied to each of these criteria may be adjusted by the operator of the Wireless Location System to suit the particular design of each system.

- 5 The candidate list of SCS's 10 and antennas 10-1 are selected using a predetermined set of criteria based, for example, upon knowledge of the types of cell sites, types of antennas at the cell sites, geometry of the antennas, and a weighting factor that weights certain antennas more than other antennas. The weighting factor takes into account knowledge of the terrain in which the Wireless Location System is operating, past
- 10 empirical data on the contribution of each antenna has made to good location estimates, and other factors that may be specific to each different WLS installation. In one embodiment, for example, the Wireless Location System may select the candidate list to include all SCS's 10 up to a maximum number of sites (`max_number_of_sites`) that are closer than a predefined maximum radius from the primary site
- 15 (`max_radius_from_primary`). For example, in an urban or suburban environment, wherein there may be a large number of cell sites, the `max_number_of_sites` may be limited to nineteen. Nineteen sites would include the primary, the first ring of six sites surrounding the primary (assuming a classic hexagonal distribution of cell sites), and the next ring of twelve sites surrounding the first ring. This is depicted in Figure 9. In
- 20 another embodiment, in a suburban or rural environment, `max_radius_from_primary` may be set to 40 miles to ensure that the widest possible set of candidate SCS/antennas is available. The Wireless Location System is provided with means to limit the total number of candidate SCS's 10 to a maximum number (`max_number_candidates`), although each candidate SCS may be permitted to choose the best port from among its
- 25 available antennas. This limits the maximum time spent by the Wireless Location System processing a particular location. `Max_number_candidates` may be set to thirty-two, for example, which means that in a typical three sector wireless communications system with diversity, up to $32 * 6 = 192$ total antennas could be considered for location processing for a particular transmission. In order to limit the time spent processing a
- 30 particular location, the Wireless Location System is provided with means to limit the number of antennas used in the location processing to `max_number_antennas_processed`.

Max_number_antennas_processed is generally less than max_number_candidates, and is typically set to sixteen.

- While the Wireless Location System is provided with the ability to dynamically
- 5 determine the candidate list of SCS's 10 and antennas based upon the predetermined set of criteria described above, the Wireless Location System can also store a fixed candidate list in a table. Thus, for each cell site and sector in the wireless communications system, the Wireless Location System has a separate table that defines the candidate list of SCS's 10 and antennas 10-1 to use whenever a wireless transmitter
- 10 initiates a transmission in that cell site and sector. Rather than dynamically choose the candidate SCS/antennas each time a location request is triggered, the Wireless Location System reads the candidate list directly from the table when location processing is initiated.
- 15 In general, a large number of candidate SCS's 10 is chosen to provide the Wireless Location System with sufficient opportunity and ability to measure and mitigate multipath. On any given transmission, any one or more particular antennas at one or more SCS's 10 may receive signals that have been affected to varying degrees by multipath. Therefore, it is advantageous to provide this means within the Wireless
- 20 Location System to dynamically select a set of antennas which may have received less multipath than other antennas. The Wireless Location System uses various techniques to mitigate as much multipath as possible from any received signal; however it is frequently prudent to choose a set of antennas that contain the least amount of multipath.

25 Choosing Reference and Cooperating SCS/Antennas

- In choosing the set of SCS/antennas to use in location processing, the Wireless Location System orders the candidate SCS/antennas using several criteria, including for example: average SNR over the transmission interval used for location processing, the variance in the SNR over the same interval, correlation of the beginning of the received
- 30 transmission against a pure pre-cursor (i.e. for AMPS, the dotting and Barker code) and/or demodulated data from the primary SCS/antenna, the time of the on-set of the transmission relative to the on-set reported at the SCS/antenna at which the transmission

was demodulated, and the magnitude and rate of change of the SNR from just before the on-set of the transmission to the on-set of the transmission, as well as other similar parameters. The average SNR is typically determined at each SCS, and for each antenna in the candidate list either over the entire length of the transmission to be used for location processing, or over a shorter interval. The average SNR over the shorter interval can be determined by performing a correlation with the dotting sequence and/or Barker code and/or sync word, depending on the particular air interface protocol, and over a short range of time before, during, and after the timestamp reported by the primary SCS 10. The time range may typically be +/- 200 microseconds centered at the timestamp, for example. The Wireless Location System will generally order the candidate SCS/antennas using the following criteria, each of which may be weighted when combining the criteria to determine the final decision: average SNR for a given SCS/antenna must be greater than a predetermined threshold to be used in location processing; SCS/antennas with higher average SNR are preferred over those with lower average SNR; SCS/antennas with lower SNR variance are preferred to those with higher SNR variance; SCS/antennas with an on-set closer to the on-set reported by the demodulating SCS/antenna are preferred to those with an on-set more distant in time; SCS/antennas with a faster SNR rate of change are preferred to those with a slower rate of change; SCS/antennas with lower incremental weighted GDOP are preferred over those with higher incremental weighted GDOP, wherein the weighting is based upon estimated path loss from the primary SCS. The weighting applied to each of these preferences may be adjusted by the operator of the Wireless Location System to suit the particular design of each system. The number of different SCS's 10 used in the location processing is maximized up to a predetermined limit; the number of antennas used at each SCS 10 is limited to a predetermined limit; and the total number of SCS/antennas used is limited to max_number_antennas_processed. The SCS/antenna with the highest ranking using the above described process is designated as the reference SCS/antenna for location processing.

30 Best Port Selection Within an SCS 10

Frequently, the SCS/antennas in the candidate list or in the list to use in location processing will include only one or two antennas at a particular SCS 10. In these cases,

the Wireless Location System may permit the SCS 10 to choose the “best port” from all or some of the antennas at the particular SCS 10. For example, if the Wireless Location System chooses to use only one antenna at a first SCS 10, then the first SCS 10 may select the best antenna port from the typical six antenna ports that are connected to that SCS 10, or it may choose the best antenna port from among the two antenna ports of just one sector of the cell site. The best antenna port is chosen by using the same process and comparing the same parameters as described above for choosing the set of SCS/antennas to use in location processing, except that all of the antennas being considered for best port are all in the same SCS 10. In comparing antennas for best port, the SCS 10 may also optionally divide the received signal into segments, and then measure the SNR separately in each segment of the received signal. Then, the SCS 10 can optionally choose the best antenna port with highest SNR either by (i) using the antenna port with the most segments with the highest SNR, (ii) averaging the SNR in all segments and using the antenna port with the highest average SNR, or (iii) using the antenna port with the highest SNR in any one segment.

Detection and Recovery From Collisions

Because the Wireless Location System will use data from many SCS/antenna ports in location processing, there is a chance that the received signal at one or more particular SCS/antenna ports contains energy that is co-channel interference from another wireless transmitter (i.e. a partial or full collision between two separate wireless transmissions has occurred). There is also a reasonable probability that the co-channel interference has a much higher SNR than the signal from the target wireless transmitter, and if not detected by the Wireless Location System, the co-channel interference may cause an incorrect choice of best antenna port at an SCS 10, reference SCS/antenna, candidate SCS/antenna, or SCS/antenna to be used in location processing. The co-channel interference may also cause poor TDOA and FDOA results, leading to a failed or poor location estimate. The probability of collision increases with the density of cell sites in the host wireless communications system, especially in dense suburban or rural environments where the frequencies are re-used often and wireless usage by subscribers is high.

Therefore, the Wireless Location System includes means to detect and recover from the types of collisions described above. For example, in the process of selecting a best port, reference SCS/antenna, or candidate SCS/antenna, the Wireless Location System determines the average SNR of the received signal and the variance of the SNR over the interval of the transmission; when the variance of the SNR is above a predetermined threshold, the Wireless Location System assigns a probability that a collision has occurred. If the signal received at an SCS/antenna has increased or decreased its SNR in a single step, and by an amount greater than a predetermined threshold, the Wireless Location System assigns a probability that a collision has occurred. Further, if the average SNR of the signal received at a remote SCS is greater than the average SNR that would be predicted by a propagation model, given the cell site at which the wireless transmitter initiated its transmission and the known transmit power levels and antenna patterns of the transmitter and receive antennas, the Wireless Location System assigns a probability that a collision has occurred. If the probability that a collision has occurred is above a predetermined threshold, then the Wireless Location System performs the further processing described below to verify whether and to what extent a collision may have impaired the received signal at an SCS/antenna. The advantage of assigning probabilities is to reduce or eliminate extra processing for the majority of transmissions for which collisions have not occurred. It should be noted that the threshold levels, assigned probabilities, and other details of the collision detection and recovery processes described herein are configurable, i.e., selected based on the particular application, environment, system variables, etc., that would affect their selection.

For received transmissions at an SCS/antenna for which the probability of a collision is above the predetermined threshold and before using RF data from a particular antenna port in a reference SCS/antenna determination, best port determination or in location processing, the Wireless Location System preferably verifies that the RF data from each antenna port is from the correct wireless transmitter. This is determined, for example, by demodulating segments of the received signal to verify, for example, that the MIN, MSID, or other identifying information is correct or that the dialed digits or other message characteristics match those received by the SCS/antenna that initially demodulated the transmission. The Wireless Location System may also correlate a short

- segment of the received signal at an antenna port with the signal received at the primary SCS 10 to verify that the correlation result is above a predetermined threshold. If the Wireless Location System detects that the variance in the SNR over the entire length of the transmission is above a pre-determined threshold, the Wireless Location System may
- 5 divide the transmission into segments and test each segment as described herein to determine whether the energy in that segment is primarily from the signal from the wireless transmitter for which location processing has been selected or from an interfering transmitter.
- 10 The Wireless Location System may choose to use the RF data from a particular SCS/antenna in location processing even if the Wireless Location System has detected that a partial collision has occurred at that SCS/antenna. In these cases, the SCS 10 uses the means described above to identify that portion of the received transmission which represents a signal from the wireless transmitter for which location processing has been
- 15 selected, and that portion of the received transmission which contains co-channel interference. The Wireless Location System may command the SCS 10 to send or use only selected segments of the received transmission that do not contain the co-channel interference. When determining the TDOA and FDOA for a baseline using only selected segments from an SCS/antenna, the Wireless Location System uses only the
- 20 corresponding segments of the transmission as received at the reference SCS/antenna. The Wireless Location System may continue to use all segments for baselines in which no collisions were detected. In many cases, the Wireless Location System is able to complete location processing and achieve an acceptable location error using only a portion of the transmission. This inventive ability to select the appropriate subset of the
- 25 received transmission and perform location processing on a segment by segment basis enables the Wireless Location System to successfully complete location processing in cases that might have failed using previous techniques.

Multiple Pass Location Processing

- 30 Certain applications may require a very fast estimate of the general location of a wireless transmitter, followed by a more accurate estimate of the location that can be sent subsequently. This can be valuable, for example, for E9-1-1 systems that handle wireless

calls and must make a call routing decision very quickly, but can wait a little longer for a more exact location to be displayed upon the E9-1-1 call-taker's electronic map terminal. The Wireless Location System supports these applications with an inventive multiple pass location processing mode.

5

In many cases, location accuracy is enhanced by using longer segments of the transmission and increasing the processing gain through longer integration intervals. But longer segments of the transmission require longer processing periods in the SCS 10 and TLP 12, as well as longer time periods for transmitting the RF data across the communications interface from the SCS 10 to the TLP 12. Therefore, the Wireless Location System includes means to identify those transmissions that require a fast but rough estimate of the location followed by more complete location processing that produces a better location estimate. The Signal of Interest Table includes a flag for each Signal of Interest that requires a multiple pass location approach. This flag specifies the maximum amount of time permitted by the requesting location application for the first estimate to be sent, as well as the maximum amount of time permitted by the requesting location application for the final location estimate to be sent. The Wireless Location System performs the rough location estimate by selecting a subset of the transmission for which to perform location processing. The Wireless Location System may choose, for example, the segment that was identified at the primary SCS/antenna with the highest average SNR. After the rough location estimate has been determined, using the methods described earlier, but with only a subset of the transmission, the TLP 12 forwards the location estimate to the AP 14, which then forwards the rough estimate to the requesting application with a flag indicating that the estimate is only rough. The Wireless Location System then performs its standard location processing using all of the aforementioned methods, and forwards this location estimate with a flag indicating the final status of this location estimate. The Wireless Location System may perform the rough location estimate and the final location estimate sequentially on the same DSP in a TLP 12, or may perform the location processing in parallel on different DSP's. Parallel processing may be necessary to meet the maximum time requirements of the requesting location applications. The Wireless Location System supports different maximum time requirements from different location applications for the same wireless transmission.

Very Short Baseline TDOA

The Wireless Location System is designed to operate in urban, suburban, and rural areas. In rural areas, when there are not sufficient cell sites available from a single wireless carrier, the Wireless Location System can be deployed with SCS's 10 located at the cell sites of other wireless carriers or at other types of towers, including AM or FM radio station, paging, and two-way wireless towers. In these cases, rather than sharing the existing antennas of the wireless carrier, the Wireless Location System may require the installation of appropriate antennas, filters, and low noise amplifiers to match the frequency band of the wireless transmitters of interest to be located. For example, an AM radio station tower may require the addition of 800 MHz antennas to locate cellular band transmitters. There may be cases, however, wherein no additional towers of any type are available at reasonable cost and the Wireless Location System must be deployed on just a few towers of the wireless carrier. In these cases, the Wireless Location System supports an antenna mode known as very short baseline TDOA. This antenna mode becomes active when additional antennas are installed on a single cell site tower, whereby the antennas are placed at a distance of less than one wavelength apart. This may require the addition of just one antenna per cell site sector such that the Wireless Location System uses one existing receive antenna in a sector and one additional antenna that has been placed next to the existing receive antenna. Typically, the two antennas in the sector are oriented such that the primary axes, or line of direction, of the main beams are parallel and the spacing between the two antenna elements is known with precision. In addition, the two RF paths from the antenna elements to the receivers in the SCS 10 are calibrated.

25 In its normal mode, the Wireless Location System determines the TDOA and FDOA for pairs of antenna that are separated by many wavelengths. For a TDOA on a baseline using antennas from two different cell sites, the pairs of antennas are separated by thousands of wavelengths. For a TDOA on a baseline using antennas at the same cell site, the pairs of antennas are separated by tens of wavelengths. In either case, the TDOA determination effectively results in a hyperbolic line bisecting the baseline and passing through the location of the wireless transmitter. When antennas are separated by multiple

wavelengths, the received signal has taken independent paths from the wireless transmitter to each antenna, including experiencing different multipath and Doppler shifts. However, when two antennas are closer than one wavelength, the two received signals have taken essentially the same path and experienced the same fading, multipath, and Doppler shift. Therefore, the TDOA and FDOA processing of the Wireless Location System typically produces a Doppler shift of zero (or near-zero) hertz, and a time difference on the order of zero to one nanosecond. A time difference that short is equivalent to an unambiguous phase difference between the signals received at the two antennas on the very short baseline. For example, at 834 MHz, the wavelength of an AMPS reverse control channel transmission is about 1.18 feet. A time difference of 0.1 nanoseconds is equivalent to a received phase difference of about 30 degrees. In this case, the TDOA measurement produces a hyperbola that is essentially a straight line, still passing through the location of the wireless transmitter, and in a direction that is rotated 30 degrees from the direction of the parallel lines formed by the two antennas on the very short baseline. When the results of this very short baseline TDOA at the single cell site are combined with a TDOA measurement on a baseline between two cell sites, the Wireless Location System can determine a location estimate using only two cell sites.

Monitoring of Call Information

20 *Overview*

A network-based WLS uses geographically separated receivers to listen for signals from a roving transmitter. In a wireless communications network, the roving transmitter, in this case a wireless phone, can be broadcasting on any one of potentially thousands of control or traffic channels. A mechanism is needed for collecting this channel and caller information. We will now describe the subject invention, which provides a mechanism for communicating with the wireless system with minimal impact to the existing system by passively monitoring a specific link for cell ID, timing advance or PN offset, frequency, caller information and other information specific to a subscriber. (This is alluded to above in connection with the description of the AP – see the subsection titled "Monitor Internal Wireless Communications System Interfaces, State Table.") The specific link, e.g., may be the BSC-BTS link called the "Abis" link in GSM and other names by various manufacturers for other radio access system (AMPS,

CDMA, TDMA, PDC, J-CDMA, CDMAOne, CDMA2000, W-CDMA, etc.). This information obtained from the link is passed to a TDOA, AOA, or hybrid TDOA/AOA - based location system that uses the information to acquire and process wireless phone signals for the purposes of location estimation.

5

Figure 10 schematically depicts a system in which a Base Transceiver Site (BTS) 10-1 is coupled to a Base Station Controller (BSC) 10-3 by way of an Abis interface. As shown, an Abis monitor 10-2 is coupled to the Abis interface. This aspect of the present invention is described in greater detail below. Figure 10 further depicts a Mobile
 10 Switching Center (MSC) 10-4 coupled to the BSC via an "A interface", as well as a Visitor Location Register (VLR) 10-5 and Home Location Register (HLR) 10-6. The BTS, BSC, MSC, VLR and HLR are well known components of a GSM wireless communications system.

15 The present invention, in a presently preferred implementation, provides a mobile station (MS) management method for a WLS that is overlaid on at least a portion of a wireless communications system. The wireless communications system, as indicated above, includes BTS equipment connected to BSC equipment. The inventive method is generally illustrated by the flowchart of Figure 11, and involves:

20 monitoring the communications between at least one BTS and at least one BSC (step S110);
 extracting MS information from the monitored communications (step S112);
 forwarding the extracted MS information to the WLS (step S114);
 the WLS may then use the extracted MS information for a variety of purposes (step
 25 S116), which are outlined below.

The extracted MS information may include the mobile station identification (MSID), the called number dialed by the user of the MS, the contents of messages sent to the MS or from the MS, or frequency assignment information sent to the MS. In addition, the
 30 extracted MS information may include any of the following presently in use by the MS: the control channel, the traffic channel, the mobile directory number (MDN), the Electronic Serial Number (ESN), the Mobile Identity Number (MIN), the Mobile

Subscriber Identification (MSI), the international mobile subscriber identity (IMSI), the temporary mobile subscriber identity (TMSI), or the mobile station international ISDN number (MSISDN).

- 5 As mentioned, there are a number of different uses for the extracted information. First, the WLS may use the extracted information to determine whether to perform location processing for the MS, or to determine which radio resources to use in performing location processing for the MS. In addition, the WLS may store the extracted MS information in a database for use at a later time or by other applications. Preferably, the
- 10 WLS will remove the extracted MS information from the database after it is no longer valid. For example, the extracted MS information may be determined to be no longer valid because the MS is no longer registered with the wireless communications system, because a predetermined period of time has expired, because a predetermined period of time has expired without an update to the extracted MS information, or because the
- 15 extracted MS information does not match any of a set of predetermined criteria. The set of predetermined criteria may include information about the identity of the MS or the number called by the user of the MS.

Detailed Description of Exemplary Embodiment for Abis Monitoring

20 1. Introduction

- A method to employ a location system of the kind described above to locate GSM mobile phones will now be described. With the architecture described herein, the WLS would not be required to detect and demodulate messages from the mobile terminal during call setup. Instead, the location system would derive call setup information from
- 25 the Abis interface between the BTS and the BSC. From the Abis interface, the location system can identify the calling party (indirectly), the called party (i.e., 911), and the TDMA/FDMA resource that is being used for a given call at any time. In the following sections, an overview of call setup in a GSM system will be presented, including relevant messages and formats. Next, an exemplary architecture for identifying and locating calls
- 30 in a GSM system is presented, followed by the high level subsystem features used to locate GSM calls.

2. Mobile Originated Call Setup in a GSM System

2.1. Call Setup-- Early Stages

The following discussion assumes that the mobile station (MS) is in the state of
5 being "normally registered" with the network. An overview of the transactions involved
in call setup emphasizing the function of the different protocol layers is presented in
Figure 12A. It should be understood that some of the layers are completely internal to
one physical subsystem, e.g., the MS, and are used more for conceptual clarification.

10 2.1.1 Channel Request

When the MS desires to originate a call, presumably a "911" call, the CC layer in
the handset presents a request to the MM layer therein, which in turn asks the Radio
Resource (RR) layer, or Layer 3, to request a radio connection. This is depicted in the top
flow line of Figure 12A. This request is transparent to the link layer (Layer 2) and is
15 simply viewed by it as a "data indication" to be transported to higher layers.

This channel request on the physical layer (Layer 1), however, has a unique format. It
uses the "Access Burst" which is a shorter burst than the regular burst. The access burst
consists of 87 channel bits, rather than the regular 147 bits, with the remainder as guard
20 time. The MS needs the extra guard time because time advance as measured and
provided to the MS by the BTS is not available on the very first instance of random
access.

The channel request message consists of only 8 information bits. These are then coded
25 with a combination of a rate $\frac{1}{2}$ convolutional code and a 6-parity-bits cyclic code to yield
a 36-bit block. This, in turn, is augmented with a 41 bit unique training sequence, and tail
bits in the beginning and the end to create the 87-bit access burst shown in Figure 12B.

The 8 information bits in the RR layer channel request message take the form shown in
30 Figure 12C. The coding scheme for the Channel Request message is defined in
paragraph 4.6 of GSM 05.03.

The random reference is an unformatted field of variable length between two and five bits long. It is used to distinguish responses from the BTS to mobiles that may have requested radio channels simultaneously. The Establishment Cause field is also of variable length, between 3 and 6 bits long, with the generic cause of requesting a radio link. Some of the bit sequences of particular interest in this field are shown in Table 2-1, below.

Table 2-1. Some of the Channel Request Causes and their Bit Sequences (see Section 9.1.8/GSM 04.08)

Message	Establishment Cause
101xxxxx	Emergency call
111xxxxx	Originating call and TCH/F (full rate traffic channel) needed, etc.
0000xxxx	Location Updating
110xxxxx	Call re-establishment, etc.
100xxxxx, 0010xxxx 0011xxxx, 0001xxxx	Answers to paging
...	Others

As can be seen, an emergency call, whatever that is defined to be by the carrier, and whatever the handset software implements accordingly, has a unique bit pattern that could be detected. The channel request is demodulated in the BTS and passed on, in a transparent manner, via a Layer 2 "data indication" to the BSC, as a Channel Required message. The format of Channel Required message is shown in Table 2-2.

Table 2-2. Channel Required Message on the Abis Interface (Section 8.5.3/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Request Reference	9.3.19	M	TV	4
Access Delay	9.3.17	M	TV	2
Physical Context	9.3.16	O 1)	TLV	>=2

1) Optional element for additional physical channel information.

The most interesting fields here are those of the Request Reference. These are shown in more detail in Figure 12D. The RA octet is the key information octet sent by the MS in the Channel Request and would contain the random identifier and the establishment cause, e.g., bit pattern 101 for 911. The other octets contain the coding of the absolute
5 frame number modulo 42432 in which the access burst was received.

The other contents of the Channel Required message on the Abis Interface are the access delay measured by the BTS (on the access burst), and the channel number. The frame number and access delay can be used by the location system to determine the frame
10 epoch relative to GPS time, as will be explained later. All of the useful information provided by the Channel Request message on the air interface can be obtained from the Request Reference field of the Channel Required message on the Abis interface.

2.1.2 Immediate Assignment

15 Once the Channel Required message is received and processed by the BSC, it responds by activating the appropriate transceiver at the BTS to carry the SDCCH signaling channel. This is performed via the Channel Activation command. The Channel Activation command has the format and contents shown in Table 2-3 below.

20 The mandatory information in the Channel Activation command includes the Channel Number, the Activation Type, and the Channel Mode. The activation type specifies whether it is an immediate assignment or a normal assignment, a handoff, or an additional assignment (e.g., for multi-slot operation). The channel mode is of variable length and contains detailed information on the mode of the channel, i.e., speech, data or
25 signaling, its rate, speech coding algorithm, and DTX on or off.

Another information element in the Channel Activation command is the Encryption Information. This information is included only if ciphering is to be applied by the BTS, hence would be normally included in the command. The encryption information element
30 is depicted in Figure 12F. Not only does it include the algorithm but also the key (K_c) to be used for the ciphering and deciphering operations.

More information to the radio devices is provided in the Channel Activation command, including BS and MS power settings and parameters, and the timing advance.

- When the BSC receives a positive acknowledgement from the BTS via the Channel Activation Acknowledge message it sends the Immediate Assign Command to the BTS. This is used by the BTS to create the Immediate Assignment message, which is scheduled for transmission by the BTS. The Immediate Assign Command on the Abis Interface contains the complete radio definition of the physical signaling channel assigned.

10

Table 2-3. Channel Activation Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Activation Type	9.3.3	M	TV	2
Channel Mode	9.3.6	M	TLV	8-9
Channel Identification	9.3.5	O 7)	TLV	8
Encryption information	9.3.7	O 1)	TLV	>=3
Handover Reference	9.3.9	C 2)	TV	2
BS Power	9.3.4	O 3)	TV	2
MS Power	9.3.13	O 3)	TV	2
Timing Advance	9.3.24	C 3), 4)	TV	2
BS Power Parameters	9.3.32	O 5)	TLV	>=2
MS Power Parameters	9.3.31	O 5)	TLV	>=2
Physical Context	9.3.16	O 6)	TLV	>=2
SACCH Information	9.3.29	O 8)	TLV	>=3
UIC	9.3.50	C 9)	TLV	3

- 1) The Encryption Information element is only included if ciphering is to be applied.
- 2) The Handover Reference element is only included if activation type is handover.
- 3) If BS Power, MS Power and/or Timing Advance elements are present, they are to be used to set the initial transmission power and the initial L1-header.
- 4) The Timing Advance element must be included if activation type is intra cell channel change.
- 5) The BS and MS Power Parameters elements are included to indicate that BS and/or MS power control is to be performed by BTS. The maximum power to be used is indicated in the BS and MS Power elements respectively.
- 6) Optional element for additional physical channel information.
- 7) Included if compatibility with phase1 is required.

Table 2-4. Channel Activation Acknowledge (Section 8.4.2/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Frame number	9.3.8	M	TV	3

5 Table 2-5. Immediate Assign Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Full Imm. Assign Info	9.3.35	M	TV	25

10 The Immediate Assign Command also contains the Channel Number Information Element, as shown. The Channel Number contains the Channel Type, subchannel number, and the TN for all messages sent across the Abis interface. This allows correlation of and Abis message with the air interface message. The BTS sends the corresponding Layer 3 Immediate Assignment command to the MS somewhere on the CCCH. The MS needs to listen to both the CCCH and the BCCH during that period.

15

The Immediate Assignment message causes the mobile to seize the dedicated signaling channel on which it will exchange subsequent signaling messages pertaining to call setup. There are two varieties in the specification for this message. The usual Immediate Assignment, and an Immediate Assignment Extended version, which addresses
20 simultaneously two mobile stations in the same cell and provides them their dedicated signaling channel information.

For the purposes of this discussion, examining the Immediate Assignment message will suffice. (If needed in the future, the extended message version can be found in the section 9.1.19 /GSM 04.08.)

- 5 There are many important fields in the Immediate Assignment message. The “Immediate Assignment Message Type” field is just the octet: 00111111. (There are other patterns for assignment extended and rejected.) The 3-octet request reference contains first the exact content of the channel request and the rest enables the computation of the frame number (modulo 42432) in which the request was received. The channel description
- 10 contains of course critical RF information.

Table 2-6. The Radio Resource Immediate Assignment Message to the Mobile (Section 9.1.18/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
7C	L2 Pseudo Length	10.5.2.19	M	V	1
	RR management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Immediate Assignment Message Type	10.4	M	V	1
	Page Mode	10.5.2.26	M	V	1/2
	Spare Half Octet	10.5.1.8	M	V	1/2
	Channel Description	10.5.2.5	M	V	3
	Request Reference	10.5.2.30	M	V	3
	Timing Advance	10.5.2.40	M	V	1
	Mobile Allocation	10.5.2.21	M	LV	1-9
	Starting Time	10.5.2.38	O	TV	3
	IA Reset Octets (frequency parameters, before time)	10.5.2.16	M	V	0-11

15

Notes: M = Mandatory; O = Optional; V = Value; T = Type; L = Length (octet)

- In Figure 12H, TN is the timeslot number (0 to 7), TSC is the training sequence (0 to 7,
- 20 and H is the hopping indicator bit. If H = 0, no hopping is used and ARFCN is the Absolute Radio Frequency Channel Number coded in binary (0 – 1023). If H =1, then the hopping sequence is defined by MAIO (the Mobile Allocation Index Offset), and

(HSN the hopping sequence number), which takes the values 0 –63. The Mobile Allocation field and the IA rest Octets also relate to frequency hopping.

5 The Channel Description information element is defined for the Immediate Assignment message. The similarity between the Channel Description IE of the air interface and the Channel Number of the Abis messages allows correlation of Abis messages with specific physical channels on the air interface.

10 The timing advance field is a binary coded representation of the advance in bit periods required of the MS according to the measurement performed at the BTS of the received random access burst. The MS transmissions are always 3 regular burst periods behind the BTS transmission offset by the time advance specified by the BTS.

The optional starting time is again in TDMA FN units (modulo 42432). The frame is approximately 4.615 ms (8 bursts).

15 The Immediate Assign command on the Abis Interface contains the Immediate Assign message to be transmitted on the air interface. Thus, it contains three very key information elements related to a 911 call in the immediate assignment: the Request Reference (containing the bit pattern corresponding to emergency call), the Channel
20 Description, and the Mobile Allocation. This is all the information the location system needs to track the signaling channel used during the setup process of a 911 call.

2.1.3. CM Service Request

25 Once the MS receives the Immediate Assignment from the BTS, it adjusts its radio and aligns its timing then transmits back to the BTS on the specified dedicated (logical) channel the Connection Management (CM) Service Request. (That assumes, as mentioned earlier, that the MS was in the proper registered idle state). The CM service request message is synthesized and stored in the handset when the caller initiates the call sequence.

30 At the link layer, the CM service request is carried inside the SABM (Set Asynchronous Balanced Mode) Layer –2 frame, which basically enables the exchange and

acknowledgment of MS-unique information between the MS and BTS, thus avoiding any potential MS ambiguity during the random access contention phase. First, the CM service request message contains important information that can be very useful to an E-911 location system.

5

Table 2-7. Contents of the CM Service Request Message from the MS (Table 9.45/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Mobility Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	CM Service Request Message Type	10.4	M	V	1
	CM Service Type	10.5.3.3	M	V	1/2
	Ciphering Key Sequence Number	10.5.1.2	M	V	1/2
	Mobile Station Classmark	10.5.1.6	M	LV	4
	Mobile Identity	10.5.1.4	M	LV	2-9

10

The CM service request message type octet belongs to the family of mobility management message types and is 0x100100. The CM Service Type half octet carries information that could of key importance to an E-911 location system. The half byte structure and content is shown in Figure 12I.

15

The half octet pertaining to the ciphering key sequence number contain three bits that provide the network with one of seven possible sequence numbers for, or a 111 pattern which indicates that no key is present in the MS.

20

The MS "classmark 2" message is depicted in Figure 12J. It carries information on maximum RF power capability of the MS: The MS classmark 2 message also carries information on the encryption algorithm A5/x the MS supports (if any). The length of the message is variable and varies up to four octets total (only L and V are transmitted).

Finally, the important mobile identity fields are transmitted to conclude the CM Service request message from the MS. There are three types of MS identity that could be used.

These are:

- 5 TMSI: Temporary Mobile Subscriber Identity;
- IMSI: International Mobile Subscriber Identity; and
- IMEI: International Mobile Station Equipment Identity.

Relaying this information to the network is done through the Mobile Identity fields, which can be 2 to 9 octets long, and are illustrated in Figure 12K. The type of MS
10 identity used is provided in octet 3.

There are certain rules in the specification on the use of the different identity types available. For mobile originating calls, for other than “emergency” call establishment or re-establishment the priority will be for the MS to use:

- 1 1. TMSI if available,
- 15 2. IMSI if no TMSI is available.

In the case of emergency call establishment or re-establishment, a third priority is added:

- 3. IMEI is used if neither a TMSI nor an IMSI is available, or if there is no SIM, or the MS does not consider the SIM valid.

20 The actual coding of the IMSI or IMEI can be found in the specification in Section 10.5.1.4/GSM 04.08.

When the CM Service Request message (carried in the SABM frame) is received at he
25 BTS, it is sent back to the MS without any modification but encapsulated inside a UA (Unnumbered acknowledgement) frame. This takes place on the DCCH radio channel specified earlier in the Immediate Assignment.

The BTS simultaneously passes the CM Service Request to the BSC in an RR Establish
30 Indication message over the Abis interface. The particulars (e.g., radio attributes) of the mobile are stored in the BTS and/or BSC for later use. The Establishment Indication can be identified as an SDCCH message by the link Identifier. The BSC at this point establishes an SCCP (Signal Connection Control Part) connection on the A-Interface to the MSC. The CM Service Request message may be optionally piggybacked on the

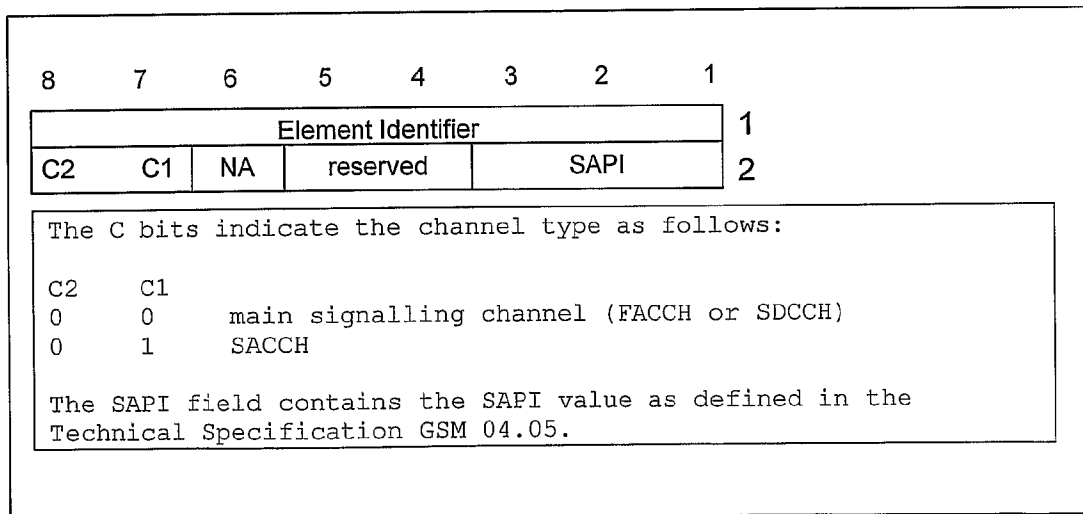
SCCP Connection Request message. It may also be sent after the SCCP connection establishment via a BSSMAP Complete Layer 3 Information message.

5 Table 2-9. Establishment Indication Message Carrying the Service Request on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Link Identifier	9.3.2	M	TV	2
L3 Information	9.3.11	O 1)	TLV	3-23

- 1) The L3 Information field is present only if the SABM frame contained a non-empty information field.

Table 2-10 Link Identifier Information Element (Section 9.3.2/GSM 08.58)



- Now, after being informed by the BSC of the existing service request, which contains the mobile subscriber's specifics, the MSC becomes involved and has the information to trigger the actions in the upper layers (MM and CC). The MSC now takes charge of the ensuing characteristics of the RR session and initiates the appropriate steps of authentication, encryption, call routing, and so on. Because the full CM Service Request message is sent across the Abis interface, the calling party's identity can be obtained from the Abis interface.

2.2 Authentication

The previous section has dealt with the early phase of call set-up, mostly that of radio resource assignment. The protocol layers involved are 1 through 3: physical, data
 5 link, and radio resource link. Before a call setup can go further, certain verification/security procedures need to be executed and these generally belong to the class of mobility management. This can be thought of as Layer 4 of the protocol stack.

The network may trigger the authentication of the PCS user identity when the user
 10 applies for:

- a change of a subscriber-related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service),
- an access to a service (including some or all of: set-up of mobile originating or
 15 terminated calls, activation or deactivation of a supplementary service), or
- first network access after restart of MSC/VLR, or in the event of cipher key sequence number mismatch.

The authentication procedure includes the following exchange between the network and
 20 the MS. The Network transmits and Authentication Request Message. The user terminal performs some computation and replies with the Authentication Response Message shown in Table 2-12.

Table 2-12. Authentication Response Message Contents

25

IEI	Information Element	Reference	Presence	Format	Length
	Mobility Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Authentication Response Message Type	10.4	M	V	1
	Authentication parameter SRES	10.5.3.2	M	V	4

2.3 Encryption/Ciphering

Although the subscriber identity and dialed digits can be determined from the Abis interface, it may be required for the location system to be able to recreate the channel bits transmitted by the mobile terminal for station based location processing. In order to create bits transmitted by the mobile, the location system may need to know of the encryption algorithm, key, and synchronization. To maintain the confidentiality of signaling and user data over the radio link, four items may have to be specified: encryption method; key setting; starting of the encryption and decryption processes; and synchronization. The encryption algorithm is known as A5.

10 Mutual key setting is the procedure that allows the MS and the network to agree on the key Kc to be used in the encryption and decryption algorithm A5. Key setting is triggered by the authentication procedure. A key setting must occur on a DCCH not yet encrypted and as soon as the identity of the mobile user (TMSI or IMSI) is known by the network.

15 Because of the potential inconsistencies that could exist between the "current" Kc on the MS and network sides, the parameter Ciphering Key Sequence Number alluded to earlier is included in the location update request and CM service request. This number is stored with the Kc, if it is found to be inconsistent upon the receipt of, say, a CM service request, the MSC/VLR knows that an authentication procedure is required before ordering the ciphered mode.

Returning to the mechanics of encryption, the operation takes place just before modulation and after interleaving; symmetrically, the decryption takes place after the demodulation. The encryption and decryption start at different instances.

The ciphering and deciphering operations are performed by applying an exclusive-or operation between the 114 coded bits of a radio burst and 114-bit ciphering sequences generated by A5 as depicted in Figure 12M. The two link directions use different sequences: for each burst, one sequence is used for ciphering in the MS and deciphering in the BTS, whereas another is used for ciphering at the BTS and deciphering at the MS.

The use of the frame number guarantees the required synchronization of the operations. For all types of radio channels the frame number changes from burst to burst. Accordingly, each burst of a given communication in the same direction uses a different ciphering sequence. The successive values for the frame number depends on the time
 5 organization of each channel and are not necessarily consecutive.

Upon receiving the contents of the CM service request at the MSC, it initiates the procedures of authentication and ciphering. Assuming successful authentication, the MSC is now ready to start the transition of the link to the ciphered mode. Ciphering,
 10 however, is a transmission function and is performed at the BTS. The decision at the MSC therefore results in a cascade of commands and steps to execute the transition. This is illustrated in Figure 12N.

The MSC sends to the BSC a BSSMAP Cipher Mode Command on the A Interface. At
 15 the BSC the cipher mode command is encapsulated in an Encryption Command on the Abis interface. This is a non-transparent command, which contains in addition to the cipher mode command, information on the specific radio channel and the ciphering key.

20 Table 2-13. Encryption Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Encryption information	9.3.7	M	TLV	>=3
Link Identifier	9.3.2	M	TV	2
L3 Info (CIPH MOD CMD)	9.3.11	M	TLV	6

The BTS upon receiving this encryption command executes the A5 algorithm but only on the receive side. It transmits to the MS in the clear the Ciphering Mode Command message. The cipher mode setting contains a bit to identify if ciphering is to be used and
 25 three bits to specify one of the possible A5 algorithm versions. The Cipher Response half octet contains one significant bit only; it specifies whether the MS is to include its

identity, specifically its IMEI, in the confirmation response, the Ciphering Mode Complete message. The identity is included only if the IMEI was requested.

The MS upon receiving the Ciphering Mode Command on the DCCH, runs the A5
 5 algorithm and starts both ciphering and deciphering. It sends back the Ciphering Mode Complete message in the ciphered mode. When the BTS receives this and successfully decipheres it, it turns on its ciphering for subsequent transmissions. The BTS relays the Cipher Mode Complete as a data indication on the Abis Interface to the BSC. The BSC, in turn, translates that information into a MAPBSS Cipher Mode Complete message on
 10 the A-Interface to the MSC.

2.4 Call Setup-- Late Stages

After entering the ciphering mode at its end, the MS sends on the DCCH that had been assigned from the beginning the call Setup message. This message contains many
 15 types of information and can vary considerable in size depending on the requested service. For voice telephony (the case of most interest for wireless location) it is simpler in content than for data or supplementary services. The regular call setup message will be discussed first. There is also in the specification an "Emergency Setup" message, which is significantly simpler. It will be described after the more general one. The location
 20 system needs to be able to handle both cases.

The structure of the regular setup message is provided in Table 2-14. The first category of information in the setup command pertains to the bearer service capability (voice at what rate, speech coding of what version, radio channel requirement, data or fax at what
 25 rate, synchronous data or not, transcoding, and so and so forth.) This information is contained in the fields called bearer Capability 1 and 2. At least one such field is mandatory. The MS needs to specify all voice rates and versions it is capable of supporting.

30 Table 2-14. Setup Message for Mobile Originating Call (Table 9.70a/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Call Control Protocol Discriminator	10.2	M	V	1/2

	Transaction Identifier	10.3.2	M	V	1/2
	Setup Message Type	10.4	M	V	1
D-	BC Repeat Indicator	10.5.4.22	C	TV	1
04	Bearer Capability 1	10.5.4.5	M	TLV	3-10
04	Bearer Capability 2	10.5.4.5	O	TLV	3-10
1C	Facility	10.5.4.15	O	TLV	2-?
5D	Calling Party Sub-address	10.5.4.10	O	TLV	2-23
5E	Called Party BCD Number	10.5.4.7	M	TLV	3-13
6D	Called Party Sub-address	10.5.4.8	O	TLV	2-23
D-	LLC Repeat Indicator	10.5.4.22	O	TV	1
7C	Low Layer Compatibility I	10.5.4.18	O	TLV	2-15
7C	Low Layer Compatibility II	10.5.4.18	O	TLV	2-15
D-	HLC Repeat Indicator	10.5.4.22	O	TV	1
7D	High Layer Compatibility I	10.5.4.16	O	TLV	2-5
7D	High Layer Compatibility II	10.5.4.16	O	TLV	2-5
7E	User-user	10.5.4.25	O	TLV	3-35
7F	SS Version	10.5.4.24	O	TLV	2-3
A1	CLIR Suppression	10.5.4.11a	C	T	1
A2	CLIR Invocation	10.5.4.11b	O	T	1

Since the TMSI (or IMSI) has been sent earlier to the network, the calling party BCD number is optional. The called party BCD number is mandatory. It is the very first time from the beginning of the RR setup procedure that this information has been divulged. The called BCD number is 3 to 19 octets long; its structure is depicted in Figure 12P. A called party subaddress field could also be included but not usually for voice; it varies in length between 2 and 23 octets. The other optional fields in the setup message pertain to whether the MS would like to provide additional compatibility information for the lower layers, e.g., as with some possible data or supplementary services. These will likely be missing in a voice call setup.

The "Emergency Setup" message has the structure shown in Table 2-15. Obviously it does away with much unnecessary information in the case of an emergency (911) call. There are no called and calling number fields. The bearer capability is, however, included and indicates speech with the appropriate version(s) the MS supports, and the appropriate value in the radio channel requirement field. This emergency setup message can have an overall length of as little as 5 octets and as long as 12.

Table 2-15. Emergency Call Setup message Content (Section 9.3.8/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
04	Call Control Protocol Discriminator	10.2	M	V	1/2
	Transaction Identifier	10.3.2	M	V	1/2
	Emergency Setup Message Type	10.4	M	V	1
	Bearer Capability	10.5.4.5	O	TLV	3-10

- 5 The setup message is received by the BTS and forwarded transparently to the BSC as a data indication. By obtaining this data indication from the Abis interface, the location system would have access to the called party number. The BSC in turn forwards the setup message to the MSC. The MSC examines the setup message contents and analyzes the MS's request. If for some reason it cannot accept or process the call, it sends back a
- 10 message to release the link. Assuming that the MSC will service the call, it initiates whatever it needs to perform to establish the connection on the external network side and, at the same time, sends towards the MS a Call Proceeding message.

- 15 The Call Proceeding message passes transparently through the BSC and BTS and the message transmitted on the air interface. This message could be as simple and short as two octets; it serves to inform the MS that the call establishment request has been received and that no more call establishment information will be accepted (for now at least). The bearer capability fields may be used in the cases when terminal adaptation is needed (generally not applicable for voice).

- 20 At initial assignment, the transmission mode is chosen by the BSC and it includes one of the signaling only modes, in clear text. In the European GSM specification three radio assignment strategies are considered: Very Early Assignment, Early Assignment, and so-called Off-the-Air Call Setup (OACSU). In very early assignment a full rate channel is
- 25 assigned as soon as it is apparent that a voice channel is likely needed, possibly as early as the receipt of the channel request. In Early Assignment a DCCH, usually of the SDCCH/8 type, is first assigned for the duration of the signaling exchanges, and then

when it is confirmed in the setup message that a voice channel is needed, then a full rate voice radio channel is assigned. In the third strategy, OACSU, a voice radio channel is not assigned until the called party answers. This may save on radio resources but can result in the need for interim announcements after the called party answers and until the
5 radio channel is assigned.

At present, an SDCCH/8 control channel is initially assigned for signaling. More generally this could be a full rate SDCCH (basically a voice channel but in signaling mode). Subsequently, during the lifetime of the RR session, the choice of transmission
10 mode depends on the communication needs and is done by the MSC. The MSC can change the mode or channel at anytime during the RR connection, and does so via an "assignment" procedure.

In the most general case two cases exist: (1) the radio channel is to stay the same but its
15 mode is to be changed, e.g., from one type of traffic to another, and (2) a new radio channel is needed to meet the voice communication requirements. The second case is the one applicable at present. (The first case would be more consistent with Very Early Assignment.)

20 To initiate the assignment procedure, the MSC sends a BSSMAP Assignment Request message to the BSC, which performs what is sometimes called a Subsequent Assignment procedure. The BSC sends to the BTS two messages, the first is a Channel Activation command, to configure and turn on the required TRX for the new channel, and the second message is the Assignment Command to be sent on the existing DCCH. The
25 Assignment Command is used when no new time advance needs to be conveyed to the MS. With the transmission of the Assignment Command, all signaling messages not related to RR management are suspended until completion of assignment.

The Assignment Command is a transparent message as far as the BTS is concerned and
30 is sent to it as a data request. Obviously this is a key message that carries critical information if following the voice channel is of interest to the location system. However,

it also contains much additional information that is very unlikely to be encountered in the case of normal voice service, particularly emergency calls.

Important elements in the message are the description of the first channel, and the power
 5 IE. The channel description fields have been described earlier, and they contain the channel type, TN, the training sequence, and either the absolute radio frequency number or the hopping sequence parameters (HSN, MAIO). The power command octet specifies the initial power of the mobile; it has five bits that specify the binary representation of the power control level (range: 1-32).

10

The Assignment Command contains a host of other options. For example, a second channel could also be described after a certain starting time. This pertains primarily to the case when the MS will have two dedicated traffic channels; it is intended for half-rate voice. The Assignment Command could also include new frequency lists for frequency
 15 hopping. These fields could be quite long (up to 132 octets each) and their coding involved. Since frequency hopping is likely to be implemented in the future, those fields would also need to be decoded if voice channel tracking is desired.

20

When the MS receives the Assignment Command it initiates the new connection at the various layers. The new voice channel is established with its associated signaling channels, the SACCH and FACCH, which are distinct from the existing (sometimes called main) signaling channel, the DCCH, in use during the call setup. The MS waits for the starting time to start the voice connection and transmission, but if the starting time had already elapsed, it starts on the voice channel immediately as a reaction.

25

Upon completing the assignment, the MS transmits back to the BTS/BSC/MSR an Assignment Complete on the main DCCH. The Assignment Complete command transmitted over the air interface. The RR cause octet is "Normal Event" and its value is 00000000.

30

Table 2-16. Assignment Command Message Contents

IEI	Information Element	Reference	Presence	Format	Length
	RR management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Assignment Command Message Type	10.4	M	V	1
	Description of the First Channel, after time	10.5.2.5	M	V	3
	Power Command	10.5.2.28	M	V	1
05	Frequency List, after time	10.5.2.13	C	TLV	4-132
62	Cell Channel Description	10.5.2.1	O	TV	17
63	Mode of the First Channel	10.5.2.6	O	TV	2
64	Description of the Second Channel, after time	10.5.2.5	O	TV	4
66	Mode of the Second Channel	10.5.2.7	O	TV	2
72	Mobile Allocation, after time	10.5.2.21	C	TLV	3-10
7C	Starting Time	10.5.2.38	O	TV	3
19	Frequency List, before time	10.5.2.13	C	TLV	4-132
1C	Description of the First Channel, before time	10.5.2.5	O	TV	4
1D	Description of the Second Channel, before time	10.5.2.5	O	TV	4
1E	Frequency channel sequence, before time	10.5.2.12	C	TV	10
21	Mobile Allocation, before time	10.5.2.21	C	TLV	3-10
9-	Cipher Mode Setting	10.5.2.9	O	TV	1

The BTS passes the assignment complete message transparently as a data indication to
 5 the BSC. The BSC relays the corresponding MAP message on the A-Interface. The MSC
 then sends an Alerting message to the MS to indicate that the called user at the fixed end
 has been alerted. This is a short message, with possible optional information that is not
 likely to be used for normal or emergency voice calls. The Alert message is another
 transparent message passed as a data request on the Abis interface. The Alert message is
 10 sent over the air. The location system will likely have no need for the alerting message.

The MSC then sends a Connect message to indicate call acceptance by the called user.
 The basic part of this message is again short but there are options that could be many
 octets long, such as the called number and subaddress. The MS stops its local alerting, if

any, of the MS subscriber and responds with a Connect Acknowledge which is the simple two octet message. Now, finally, the MS connects the speech path to the radio channel assigned to the voice and the conversation data flows. At this point, the DCCH is relinquished with an RF Channel Release sent to the BTS, and becomes available to

5 service another call setup.

Table 2-17. RF Channel Release (Section 8.4.14/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2

10 Table 2-18. RF Channel Release Ack (Section 8.4.19/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2

3. Mobile Terminated Call setup in a GSM System

- 15 A mobile terminated call setup in a GSM system includes the following steps:
- Page from the network (Table 3-1).
 - Mobile terminal then responds with a Channel Request, with a response to page cause.
 - Immediate Assignment takes place.
 - 20 The Page Response is transmitted once the SDCCH is assigned, instead of a CM Service Request.
 - Authentication followed by encryption.
 - Network Sends a Setup Message to the Mobile terminal (Table 3-2).
 - Mobile terminal replies with a Call Confirmed Message.
 - 25 Call then completes in the same manner as a mobile originated call.

From the Abis interface, the location system can determine the identity of the called party, as well as the physical resources used by the call. This information allows the location system to identify calls of interest, and locate the mobile phone receiving that call.

5

Table 3-1. Contents of the Page Response Message from the MS (Table 9.25/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	RR Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Page Responset Message Type	10.4	M	V	1
	Ciphering Key Sequence Number	10.5.1.2	M	V	1/2
	Spare Half Octet	10.5.1.8	M	V	1/2
	Mobile Station Classmark	10.5.1.6	M	LV	4
	Mobile Identity	10.5.1.4	M	LV	2-9

10 Table 3-2. Setup Message for Mobile Terminating Call (Table 9.70/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Call Control Protocol Discriminator	10.2	M	V	1/2
	Transaction Identifier	10.3.2	M	V	1/2
	Setup Message Type	10.4	M	V	1
D-	BC Repeat Indicator	10.5.4.22	C	TV	1
04	Bearer Capability 1	10.5.4.5	O	TLV	3-10
04	Bearer Capability 2	10.5.4.5	O	TLV	3-10
1C	Facility	10.5.4.15	O	TLV	2-?
1E	Progress Indicator	10.5.4.21	O	TLV	4
34	Signal	10.5.4.23	O	TV	2
5C	Calling Party BCD Number	10.5.4.9	O	TLV	3-14
5D	Calling Party Sub-address	10.5.4.10	O	TLV	2-23
5E	Called Party BCD Number	10.5.4.7	O	TLV	3-13
6D	Called Party Sub-address	10.5.4.8	O	TLV	2-23
D-	LLC Repeat Indicator	10.5.4.22	O	TV	1
7C	Low Layer Compatibility I	10.5.4.18	O	TLV	2-15
7C	Low Layer Compatibility II	10.5.4.18	C	TLV	2-15
D-	HLC Repeat Indicator	10.5.4.22	O	TV	1
7D	High Layer Compatibility I	10.5.4.16	O	TLV	2-5
7D	High Layer Compatibility II	10.5.4.16	C	TLV	2-5

7E	User-user	10.5.4.25	O	TLV	3-35
----	-----------	-----------	---	-----	------

4. System Architecture for GSM

An illustrative system architecture for the location of GSM mobile phones is shown in Figure 12Q. The main modification to support GSM is the addition of the Abis Monitoring Subsystem (AMS). The AMS monitors the signaling links on the Abis interface. A second modification is the NSS Interface System (NIS), which obtains a mapping of the TMSI to the IMSI and MSISDN for a subscriber, and can provide a subscriber the current location in the form of a short message.

10

The AMS will continuously monitor the Layer 2 LAPD signaling links on the Abis interface, for each cell in the GSM system. The AMS will monitor the LAPD frames and identify Immediate Assign Command messages. The AMS need not monitor the Channel Required messages, because all relevant information in the Channel Required message is repeated in the Immediate Assign Command. From the Immediate Assign Command, the AMS can identify emergency calls, and a description of the radio channel used for the subsequent signaling messages.

Once the Immediate Assign Command is detected, for a particular logical channel, the Abis message processor knows a new origination has occurred, and a new call record is created. The Abis processor will then look for a CM Service Request message from the channel, which will identify the mobile subscriber. The raw bits and the mobile identity are appended to the call record. The AMS then sends an origination indicator message with a hash code to the TLP, and the TLP then sends a TDOA data request to the appropriate SCSs with the same hash code, for up to 12 bursts allocated to the mobile starting with the CM service request. The TDOA data will be cached by the SCS.

The AMS will then capture and store in the call record, all messages from that mobile until it receives the setup message. Once the setup message is received, all information is available to determine if a location should be performed. The full origination, along with the mobile transmitted bits for the first 12 bursts are sent to the TLP. Missing frames will be indicated, and fill frames should be assumed.

With the complete origination information, the TLP will determine if a position determination is required. If so, the TLP will send a TOA/FOA request to the primary SCS. The request is similar to a TDOA request, but will also provide the uncoded data bits. The primary SCS will then reply with the TOA, FOA, frequency offset, and phase corrections (if required) for each burst. The SCS will also provide SNR metrics for each burst.

The TLP will then send a TOA/FOA request to each of the SCSs, with the corrections from the primary channel. The SCSs will process the data, and reply to the TLP with TOA, and FOA. The TLP will then execute the solve algorithm, and the position is determined.

The NIS will request the IMSI and MSISDN from the VLR, when needed. The NIS will support the protocol stack for communication over the SS7 network, which allows communication with GSM VLRs, HLRs and MSCs.

Once the location is determined, the AP has the subscriber's information, and current location. If the subscriber has location service, the AP would send the location information to the NIS, along with the IMSI, MSISDN, and routing information to the subscriber's current MSC. The NIS would then forward the location information to the subscriber in the form of a short message.

The location service could be a supplementary service defined in the subscriber's information or kept in the AP database.

4.1 SCS Modifications

The SCS is not required to demodulate and identify all origination messages from the mobile phones. This will be accomplished by monitoring the Abis interface. For station based processing, the SCS may have to demodulate only the bursts used for location, if those bits cannot be completely determined from the Abis interface, in cases of voice tracking.

- The SCS would, upon the receipt of a RACH Demod Request message from the TLP, search and demodulate a Random Access (RACH) Burst. The RACH Demod Request will contain the ARFCN, a time window to search, and the contents of the RACH message to be demodulated. Upon successful demodulation and decoding of the RACH burst, the SCS may provide a RACH Demod Response message, with a time stamp to the TLP, indicating when the RACH burst occurred. If the RACH burst cannot be found, the SCS may provide an error message to the TLP, indicating that the RACH was not found.
- 10 The SCS could provide 200 kHz complex video bandwidth for TDOA data. The SCS could also provide the demodulated bits for a series of bursts upon request by the TLP, and may also provide frequency and phase corrections for each of these bursts (if necessary for accuracy). This could be sent to the other SCSs to be used for station based processing. The SCS could also provide a periodic message to the TLP, bound for the
- 15 AMS, which indicates the time drift between GPS and the T1 frame clock.

- Frame timing to the accuracy of a few microseconds can be initially determined by a search of a short burst (maybe a RACH burst) for each site in the system. This timing can then be maintained by counting the T1 frames in one of the SCSs, and calculating Tdrift. Also, the TOA could be used to update the timing with each location. Upon receipt of a call cancel message, the SCS could match the hash code with the TDOA data stored in cache, and delete that TDOA data.
- 20

4.2 TLP Modifications

- 25 The TLP could be made to accept originations from the AMS, instead of the SCSs. The origination could be sent to the TLP in 2 messages, which can be linked by a hash code. The first message is just an indication that an origination has begun, and will include a timestamp. This message allows the TLP to start the TDOA data caching process. This caching process is probably not needed, as the phone does not reduce power for several
- 30 seconds. Data can be collected once an SOI is determined, from information in the seconds message. The second message will contain all information necessary for an origination (MIN, Dialed Digits).

The TLP could also provide a link in which the AMS can request a particular SCS to demodulate a RACH burst, and provide a timestamp back to the AMS. The TLP could accept RACH Demod Request Messages from the AMS and forward them to the
5 appropriate SCS. The TLP could also Accept RACH demod response messages from the SCS and forward them to the appropriate AMS. This allows the location system to know the relative timing of each Base Stations frame epoch.

Upon receipt of a call cancel message from the AMS, the TLP would link that call cancel
10 message to the origination message, and send a call cancel message to the appropriate SCSs. The TLP will then delete the origination form its memory.

4.3 Changes to the AP

The AP could be made to have an interface to the NIS, for the purpose of sending
15 short location related messages to mobile subscribers. The functionality of the NIS could be added to the AP, making the AP to NIS an internal interface.

4.4 Abis Monitoring System (AMS)

4.4.1 Call Tracking

20 The AMS may have a connection to the Abis interface of a BSC in the GSM system. This connection may provide the AMS bi-directional monitoring access to the Abis interface for each BTS under control of the BSC. The AMS may monitor the LAPD signaling link for the beacon TRX, for each cell, to allow location upon origination of calls. The AMS architecture may expand to monitor the LAPD signaling links for each
25 TRX, for all cells controlled by the BTS, to allow location using traffic channels. The AMS architecture may allow expansion to support up to 2000 LAPD signaling links. The AMS may detect call originations through the Immediate Assign Command. The AMS may identify emergency calls from the Immediate Assign Command.

30 Upon receipt of an Immediate Assign command, the AMS may notify the appropriate TLP within 25 milliseconds. The AMS may provide to the TLP with an origination indication, including a description of the physical channel assignment, a timestamp, and

a hash code to link with the origination information later. This hash code may also permit the TLP to request current physical channel information about a particular call, after voice channel assignment. (The same hash code is used throughout the duration of the call.) This process could wait for systems in which power control does not take effect
5 for several seconds (Ericsson Omnipoint), and a single origination message could be sent to the TLP.

The AMS may detect CM Service Request, Page Response, and Location Update Request, and link them to the Immediate Assign Command for a given call setup.
10 The AMS may detect Setup messages and Link them to the Immediate Assign Command for a given call setup.

If an Immediate Assign Command for a particular physical channel is sent to the BTS
15 before all of the origination information is gathered for the previous call, the AMS may send a call cancel message to the TLP, including the same hash code used for the origination indication message.

When the AMS has the complete origination information, consisting of the physical
20 channel, Mobile identity, and dialed digits, the AMS may forward this origination information to the TLP along with the same hash code used for the origination indication.

The AMS may detect Assignment Commands and Assignment Complete responses sent
25 over Abis interface for a given call, and link them to the original Immediate Assign Message.

The AMS may detect subsequent Hand-over Commands and Hand-over Failures to maintain the most up to date physical channel assignment for a given call. (Assignment
30 commands).

The AMS may accept Physical Channel request from the TLP. The TLP will provide the unique hash code which the AMS provided with the origination. The AMS may respond with a complete description of the Physical channel currently assigned to the call, or an indication that the AMS does not have the information. This will permit voice tracking,
5 which is initiated by the TLP.

The AMS may support inter AMS communication allowing inter BSC/MSC hand-over of call records. The Hand-over Command on the Abis interface provides the new cell ID, and hence the new AMS ID. Upon successful hand-over, the AMS will append the new
10 physical channel information to the call record, and send the entire call record to the new AMS, if the call is to be serviced by a different AMS.

The AMS may support up to 160 call arrivals per second.

15 4.3.2 TRX Configuration Maintenance

The AMS may have provided to it the configuration of each TRX controlled by the BSC. The configuration is defined as the TSC, a bit to indicate if frequency hopping is applied, the MAIO and HSN if frequency hopping is applied, or the ARFCN if frequency hopping is not applied. The AMS may maintain knowledge of the TRX
20 configuration by the following algorithm:

For each Assignment Command, or Immediate Assignment command, compare the Channel Description IE to the Channel Number IE of the n most recent successful Channel Activation Commands. Successful Channel Activation Commands are defined
25 as those with a Channel Activation Ack from the BTS. If the Channel Number IE of the Channel Activation matches the matches the Channel type and TDMA offset field, and the TN field of the Channel Description IE of the Assignment or Immediate Assignment Command of any of the n Channel Activation messages, store the TSC, H, MAIO and HSN, and ARFCN fields of the Channel Description IE. The AMS should maintain a list
30 of the fields from the last m Channel Description IEs, for each TRX. When any new Channel Description IE fields are added to the list, the new TRX configuration is defined as the configuration appearing most in the list of length m. If there is a tie, then the TRX

configuration may not be updated. If there are less than m sets of configuration values, the configuration may not be updated.

The parameter n may be an operator configurable parameter with a range of 1 to 12, a step size of 1, and a default value of 2. The parameter m may be an operator configurable parameter with a range of 1 to 12, a step size of 1, and a default value of 5.

The TRX configuration should be static, and any changes in TRX configuration should be known by the location system operator some time before the change takes place.

However, if the operator is not informed, the AMS will typically learn the new configuration after $m/2+1$ calls using that TRX.

4.3.3 Synchronization Maintenance

Upon initialization the AMS may monitor the signaling links on the Abis interface [AMS] for a Channel Required message for each cell controlled by the BSC. Upon the receipt of the first Channel Required Message for a given cell, the AMS may store the frame number, $F0$, and time offset for the message, and request a timestamp determination from the TLP for that corresponding Channel Request message. In this request the AMS may include the ARFCN, a start time, and a search window length, the Channel Request message contents, and a unique hash code. The search window length, $W1$ may be an operator configurable parameter with a range of 1 to 500 milliseconds, with a step size of 1 millisecond, and a default value of 100 milliseconds. The TLP will forward this message to the appropriate SCS and eventually reply with a timestamp, and a signal quality measurement, if the burst is found, other wise, an indication that the burst was not found. If the burst was not found, the AMS repeats the process with the next Channel Required message.

When the AMS finally receives a successful timestamp for the burst, it calculates the time of the Epoch of the stored frame as GPS timestamp – Access delay, $T0$. Any subsequent frame epoch can be determined by:

$$T_{\text{frame}} = (F1 - F0) * 60 / 13 + T0.$$

The epoch for any TNx in a frame can be determined by:

$$T_{\text{frame}} + x15/26 \text{ milliseconds.}$$

Upon successful determination of the frame epoch, the AMS may start a Timer, T501.

- 5 When the timer expires, the AMS may reinitiate the epoch capture procedure. T501 may be an operator configurable parameter with a range of 1 second to 36000 seconds with a one-second-step size, and a default value of 900 seconds.

- 10 A single SCS will be configured to provide a time drift measurement, Tdrift, between the GPS time and the T1 clock. This SCS will provide a drift offset once each L seconds. Each L seconds the Tframe may be adjusted by the Tdrift. L may be an operator configurable parameter with a range of 1 to 900 seconds, step size of 1 seconds and a default value of 10 seconds.

15 4.4 NIS

The NIS could be part of the AP, and therefore need not have an explicit interface to the AP.

4.4.1 Subscriber Identification

- 20 The NIS may connect to the all VLRs in a GSM network. The NIS may connect to up to 5 VLRs. The NIS may comply with GSM 09.02 for communication with the VLR. The VLR may have a link to each AMS in the network. The NIS may support link for up to 10 AMS in the network.
- 25 The NIS may accept subscriber information request messages from each AMS in the network. The subscriber request may contain the subscriber's TMSI, or IMSI, and the VLR number with which the subscriber is registered. Upon receiving the subscriber request message, the NIS may issue a send parameters command to the appropriate VLR, and request the subscriber information. Upon successful reception of the subscriber
- 30 information from the VLR, the NIS may forward it to the requesting AMS. If the request was unsuccessful, an error message may be forwarded to the requesting AMS.

4.4.2 Short Message Service

The NIS may provide an interface to the AP. This interface will allow the AP to send short messages to a subscriber, containing the subscriber's location, or any location related data. The NIS may accept SMS requests from the AP, and forward the short messages to the appropriate MSC. Upon successful delivery of the short message, the

5 NIS may provide an acknowledgement to the AP. If the network was unsuccessful delivering the message, the NIS may inform the AP. The NIS may comply with GSM specification 09.02, when communicating with the Network.

10 Conclusion

The true scope the present invention is not limited to the presently preferred embodiments disclosed herein. For example, the foregoing disclosure of a presently preferred embodiment of a Wireless Location System uses explanatory terms, such as Signal Collection System (SCS), TDOA Location Processor (TLP), Applications

15 Processor (AP), and the like, which should not be construed so as to limit the scope of protection of the following claims, or to otherwise imply that the inventive aspects of the system are limited to the particular methods and apparatus disclosed. Moreover, as will be understood by those skilled in the art, many of the inventive aspects disclosed herein may be applied in location systems that are not based on TDOA techniques. For

20 example, the processes by which the Wireless Location System determines TDOA and FDOA values can be applied to non-TDOA systems. Similarly, the invention is not limited to systems employing SCS's constructed as described above, nor to systems employing AP's meeting all of the particulars described above. The SCS's, TLP's and AP's are, in essence, programmable data collection and processing devices that could

25 take a variety of forms without departing from the inventive concepts disclosed herein. Given the rapidly declining cost of digital signal processing and other processing functions, it is easily possible, for example, to transfer the processing for a particular function from one of the functional elements (such as the TLP) described herein to another functional element (such as the SCS or AP) without changing the inventive

30 operation of the system. In many cases, the place of implementation (i.e., the functional element) described herein is merely a designer's preference and not a hard requirement. Accordingly, except as they may be expressly so limited, the scope of protection of the

following claims is not intended to be limited to the specific embodiments described above.

CLAIMS

What is claimed is:

1. A mobile station (MS) management method for a wireless location system
5 (WLS) that estimates the geographic location of said mobile transmitter, wherein the
WLS overlays at least a portion of the geographic area of a wireless communications
system, wherein the WLS includes radio resources and location processing resources,
and wherein the wireless communications system includes base transceiver station (BTS)
equipment connected to base station controller (BSC) equipment, comprising the steps
10 of:
 continuously monitoring the communications between at least one BTS and at
least one BSC,
 extracting MS information from the monitored communications, and
 forwarding the extracted MS information to the WLS.
15
2. A method as recited in claim 1, wherein the extracted MS information may
include the mobile station identification (MSID), the called number dialed by the user of
the MS, the contents of messages sent to the MS or from the MS, or frequency
assignment information sent to the MS.
20
3. A method as recited in claim 1, wherein the extracted MS information may
include any of the following presently in use by the MS: the control channel, the traffic
channel, the mobile directory number (MDN), the Electronic Serial Number (ESN), the
Mobile Identity Number (MIN), the Mobile Subscriber Identification (MSI), the
25 international mobile subscriber identity (IMSI), the temporary mobile subscriber identity
(IMSI), or the mobile station international ISDN number (MSISDN).
4. A method as recited in claim 1, wherein the WLS uses the extracted MS
information to determine whether to perform location processing for said MS.
30

5. A method as recited in claim 1, wherein the WLS uses the extracted MS information to determine which radio resources to use in performing location processing for said MS.

5 6. A method as recited in claim 1, wherein the WLS uses the extracted MS information to determine which location processing resources to use in performing location processing for said MS.

7. A method as recited in claim 1, wherein the WLS stores the extracted MS
10 information in a database.

8. A method as recited in claim 7, wherein the WLS removes the extracted MS information from the database after the extracted MS information is no longer valid.

15 9. A method as recited in claim 8, wherein the extracted MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

10. A method as recited in claim 8, wherein the extracted MS information is
20 determined to be no longer valid because a predetermined period of time has expired.

11. A method as recited in claim 8, wherein the extracted MS information is determined to be no longer valid because a predetermined period of time has expired without an update to the extracted MS information.

25 12. A method as recited in claim 1, wherein the WLS discards the extracted MS information if the extracted MS information does not match any of a set of predetermined criteria.

30 13. A method as recited in claim 12, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

14. A method for use in a wireless location system (WLS), wherein the WLS overlays at least a portion of a wireless communications system that includes base transceiver station (BTS) equipment operatively coupled to base station controller (BSC) equipment via an interface, comprising the steps of:

5 monitoring communications on the interface between at least one BTS and at least one BSC;

identifying certain prescribed mobile station (MS) information from the monitored communications;

10 forwarding the MS information to the WLS; and

using the MS information to determine whether to perform location processing for said MS and/or to determine which radio resources to use in performing location processing for said MS and/or to determine which location processing resources to use in performing location processing for said MS.

15

15. A method as recited in claim 14, wherein the MS information includes one or more of the following: a mobile station identification (MSID), a called number, contents of messages sent to the MS or from the MS, and/or frequency assignment information sent to the MS.

20

16. A method as recited in claim 14, wherein the MS information includes one or more of the following presently in use by the MS: control channel, traffic channel, mobile directory number (MDN), Electronic Serial Number (ESN), Mobile Identity Number (MIN), Mobile Subscriber Identification (MSI), international mobile subscriber identity (IMSI), temporary mobile subscriber identity (TMSI), and/or mobile station international ISDN number (MSISDN).

25

17. A method as recited in claim 14, wherein the WLS stores the MS information in a database.

30

18. A method as recited in claim 17, wherein the WLS removes the MS information from the database after the MS information is no longer valid.

19. A method as recited in claim 18, wherein the MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

5

20. A method as recited in claim 18, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired.

21. A method as recited in claim 18, wherein the MS information is determined
10 to be no longer valid because a predetermined period of time has expired without an update to the MS information.

22. A method as recited in claim 14, wherein the WLS discards the MS
information if the MS information does not match any of a set of predetermined criteria.
15

23. A method as recited in claim 22, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

20 24. A wireless location system (WLS) that overlays at least a portion of a wireless communications system that includes base transceiver station (BTS) equipment operatively coupled to base station controller (BSC) equipment via an interface, comprising:

means for monitoring communications on the interface between at least one BTS
25 and at least one BSC;

means for identifying certain prescribed mobile station (MS) information from the monitored communications; and

means for using the MS information to determine whether to perform location processing for said MS and/or to determine which radio resources to use in performing
30 location processing for said MS and/or to determine which location processing resources to use in performing location processing for said MS.

25. A system as recited in claim 24, wherein the MS information includes one or more of the following: a mobile station identification (MSID), a called number, contents of messages sent to the MS or from the MS, and/or frequency assignment information sent to the MS.

5

26. A system as recited in claim 24, wherein the MS information includes one or more of the following presently in use by the MS: control channel, traffic channel, mobile directory number (MDN), Electronic Serial Number (ESN), Mobile Identity Number (MIN), Mobile Subscriber Identification (MSI), international mobile subscriber identity (IMSI), temporary mobile subscriber identity (TMSI), and/or mobile station international ISDN number (MSISDN).

10

27. A system as recited in claim 24, further comprising a database, wherein the WLS stores the MS information in said database.

15

28. A system as recited in claim 27, wherein the WLS removes the MS information from the database after the MS information is no longer valid.

29. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

20

30. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired.

25

31. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired without an update to the MS information.

30

32. A system as recited in claim 24, wherein the WLS discards the MS information if the MS information does not match any of a set of predetermined criteria.

33. A system as recited in claim 32, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

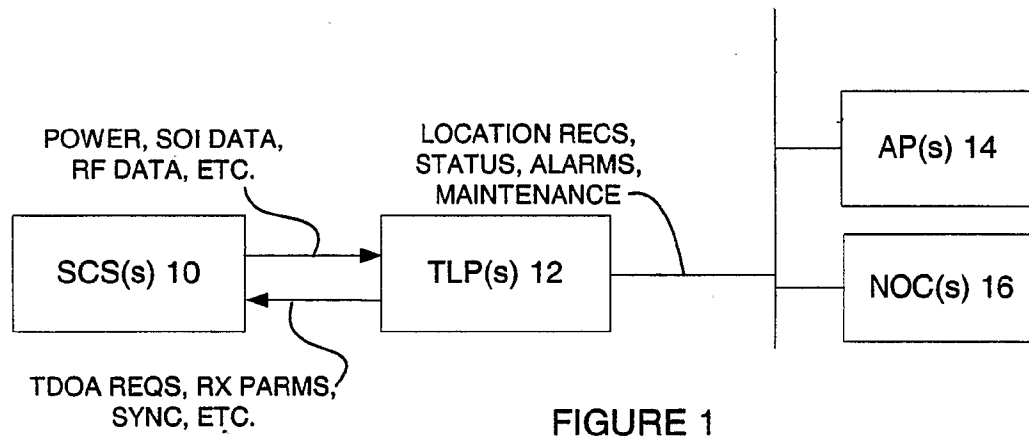


FIGURE 1

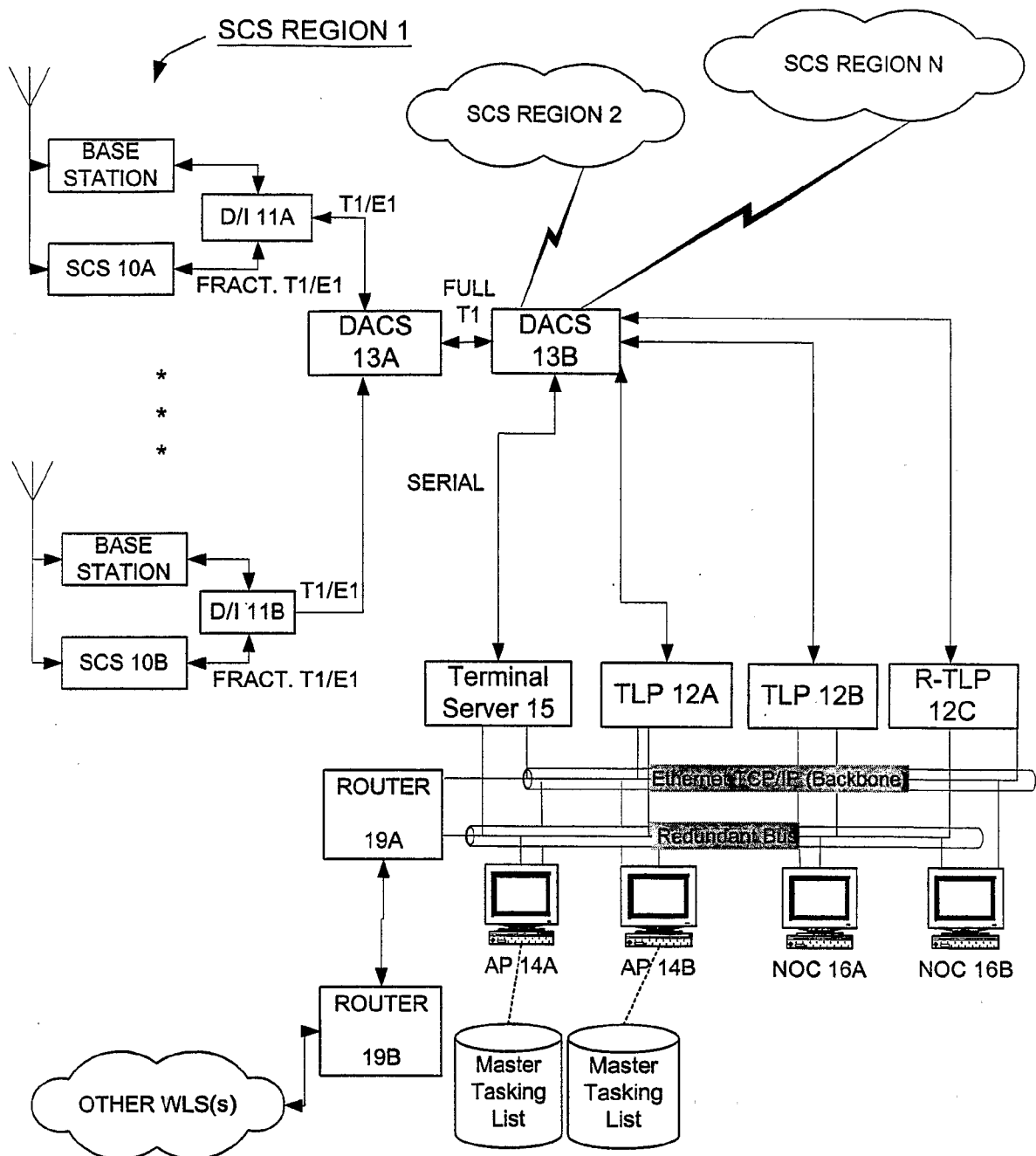


FIGURE 1A

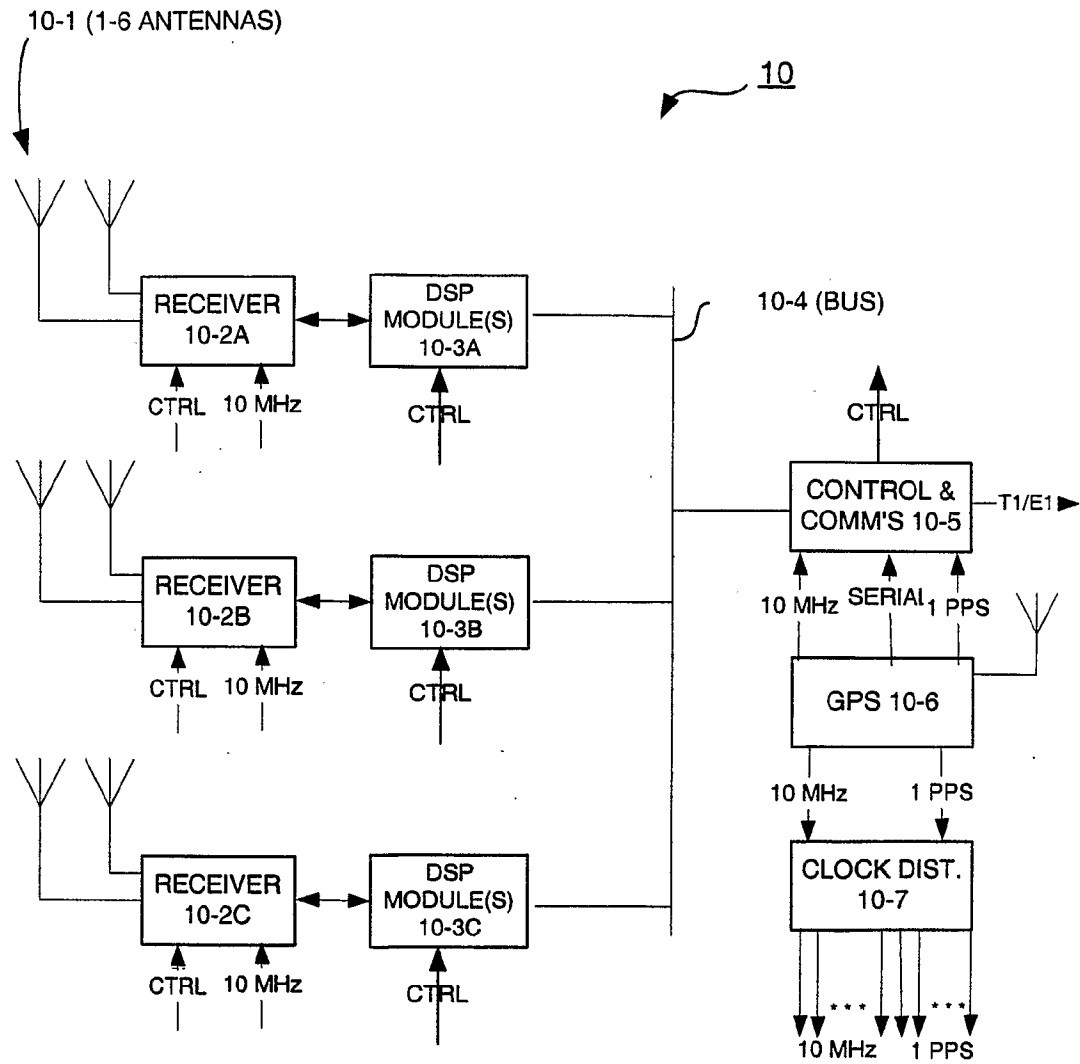


FIGURE 2

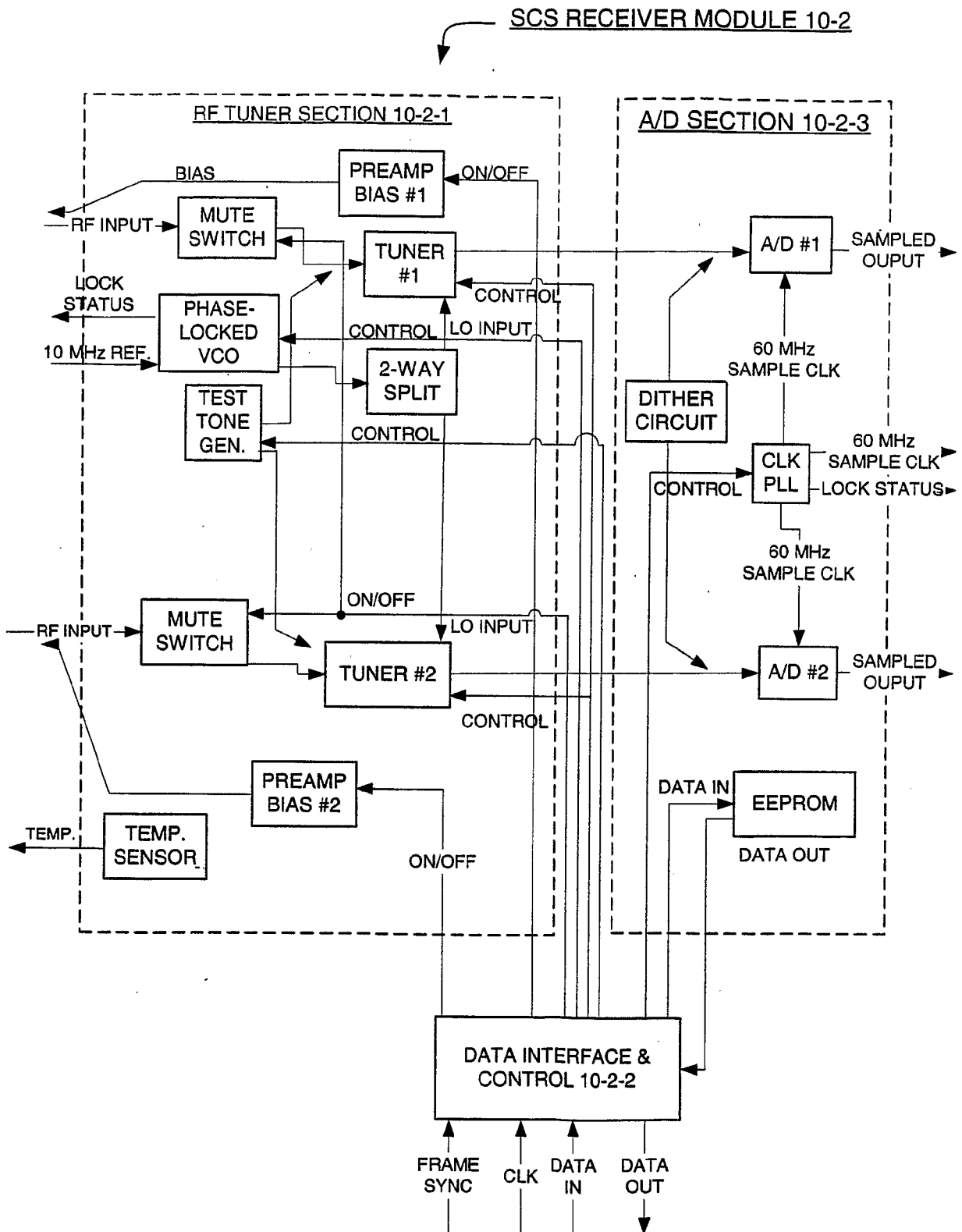


FIGURE 2A

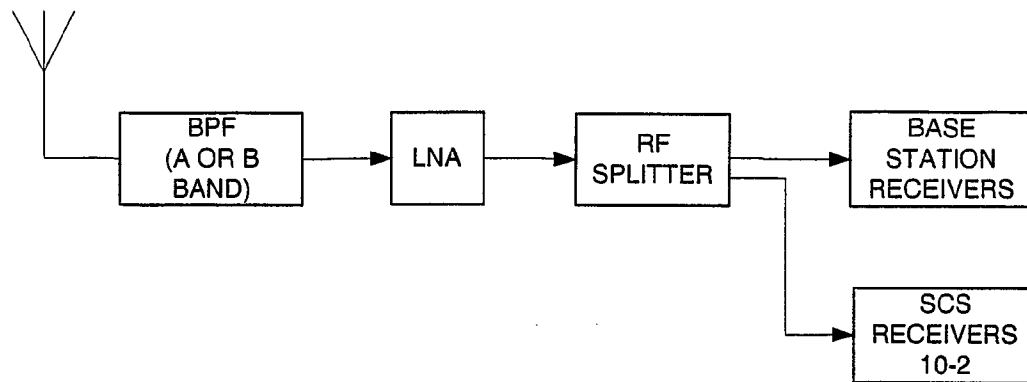


FIGURE 2B

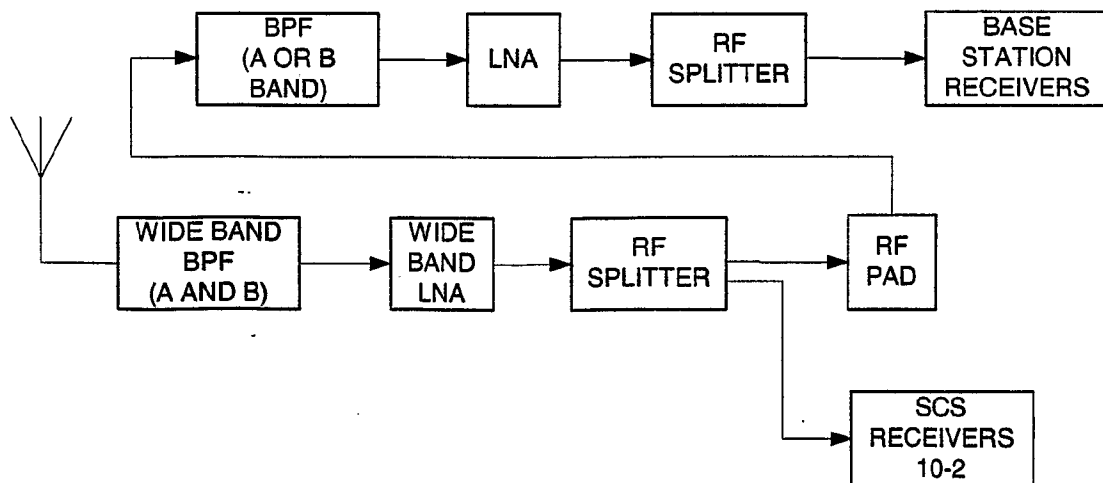


FIGURE 2C

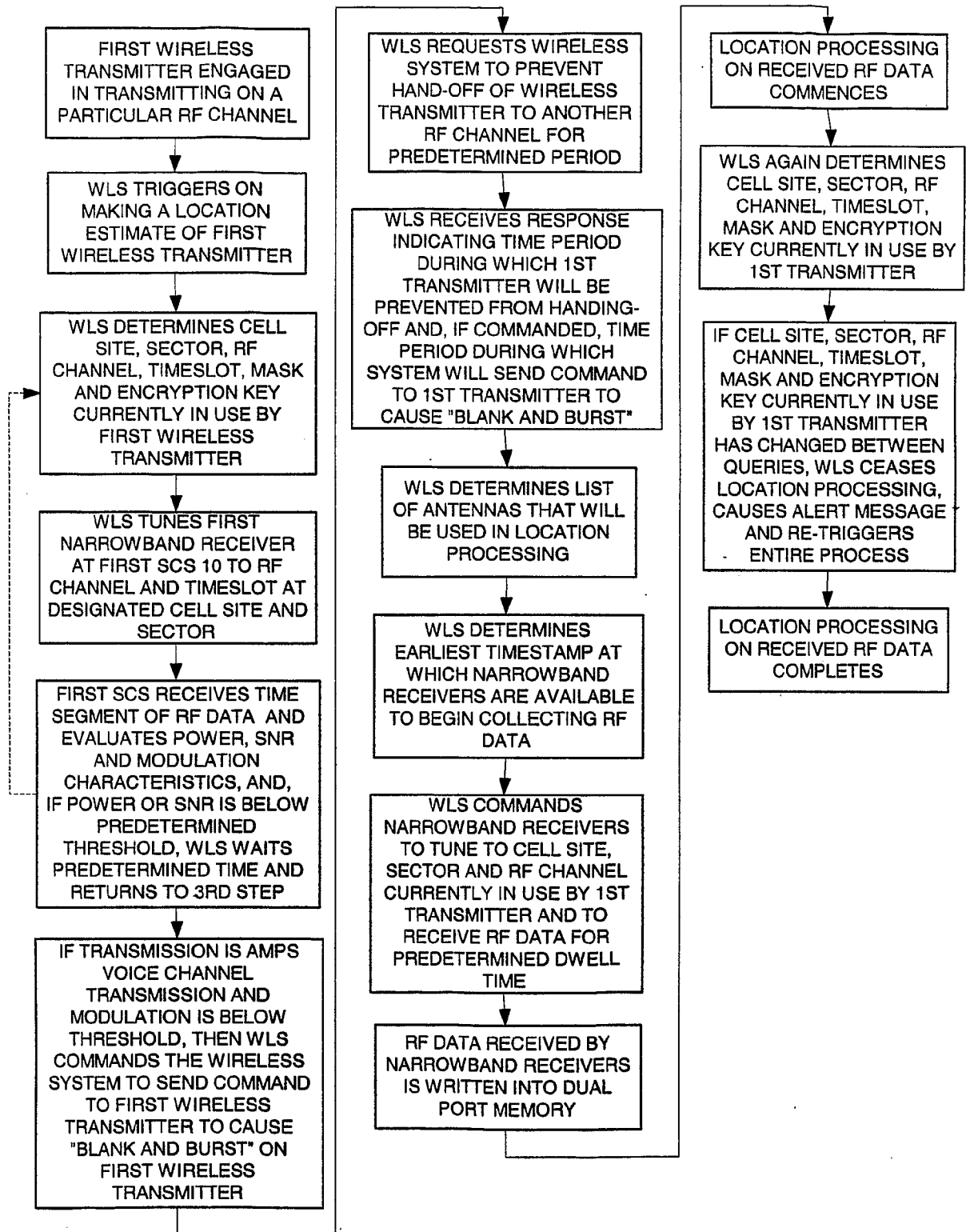


FIGURE 2C-1

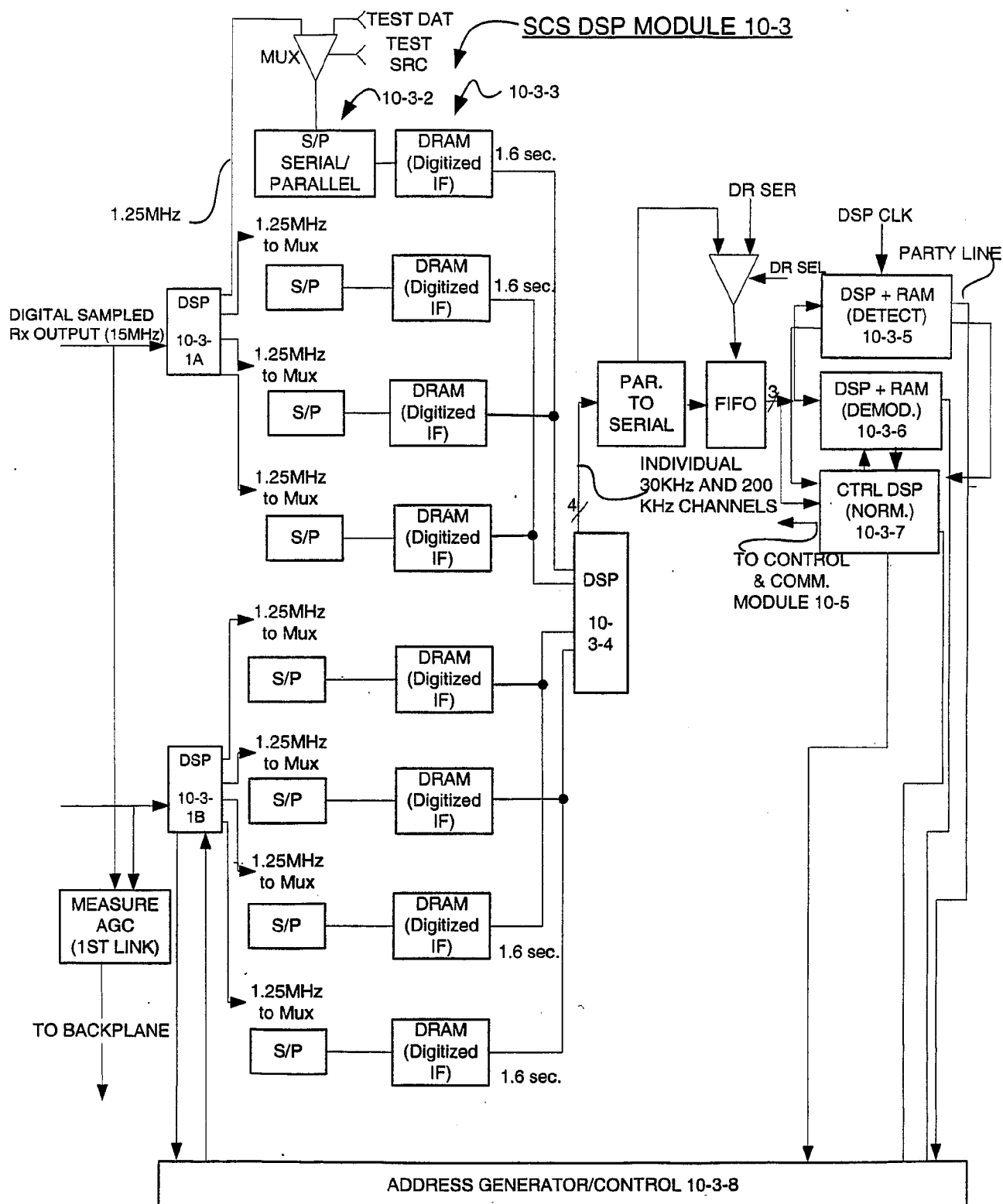


FIGURE 2D

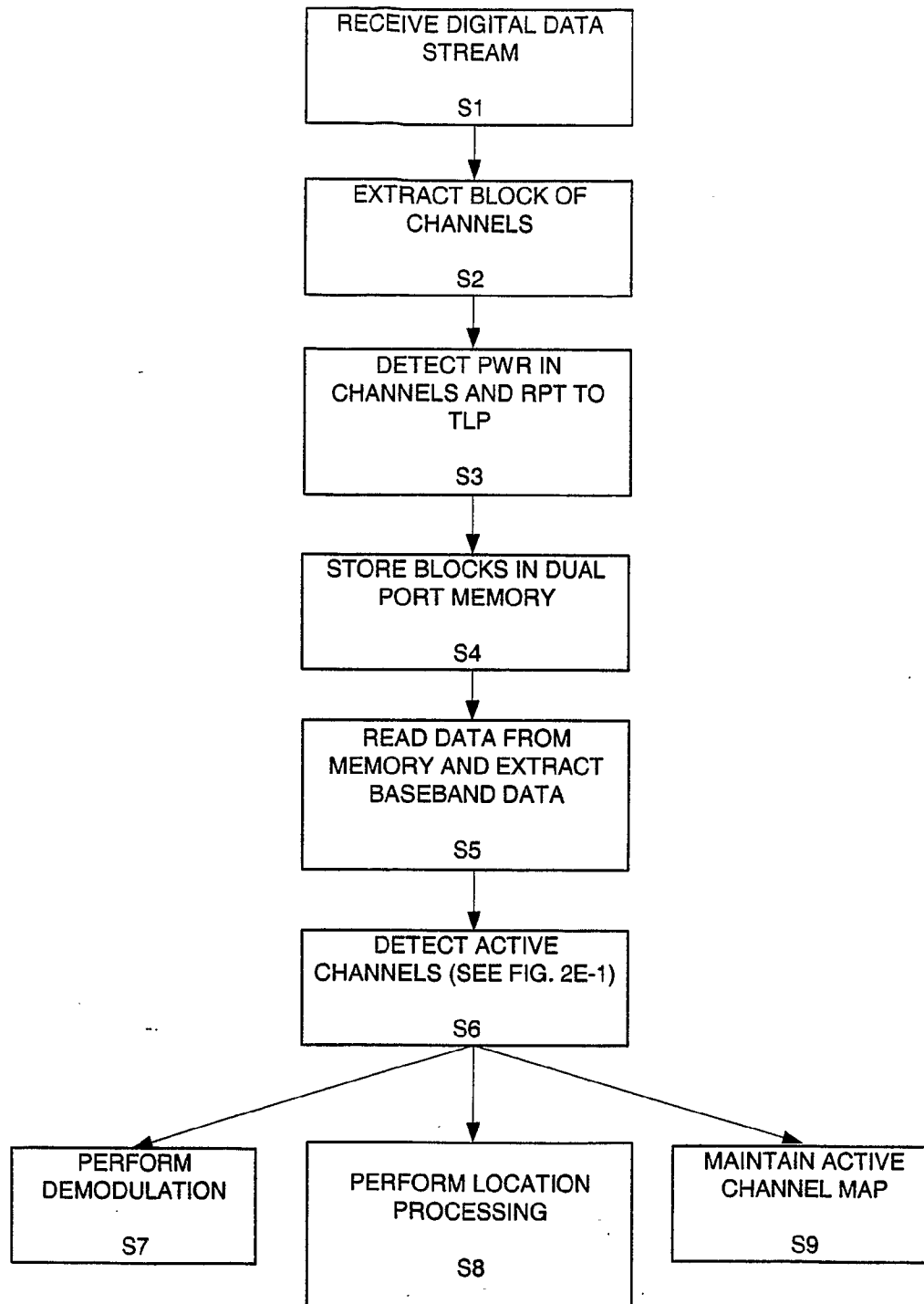


FIGURE 2E

9/31

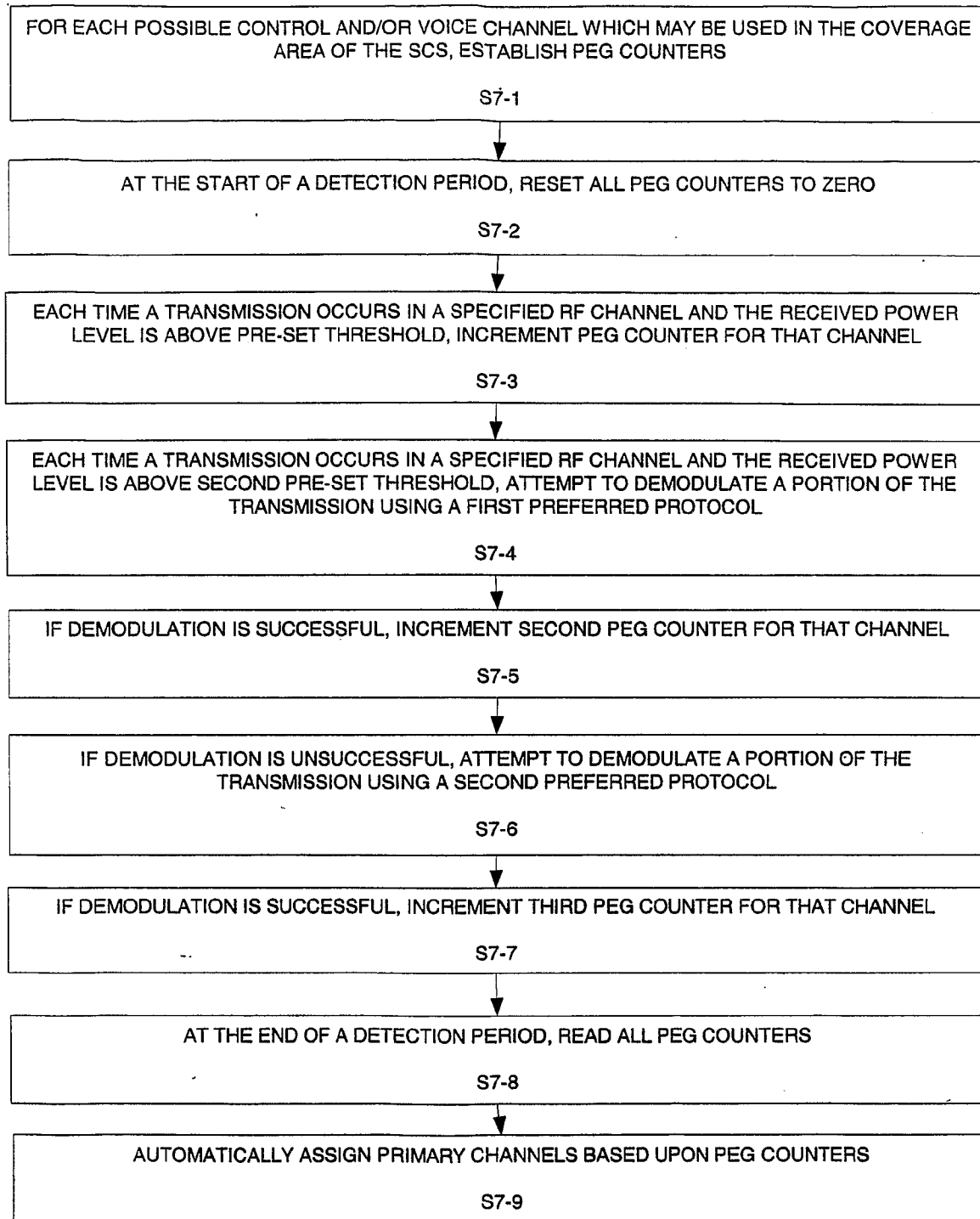


FIGURE 2E-1

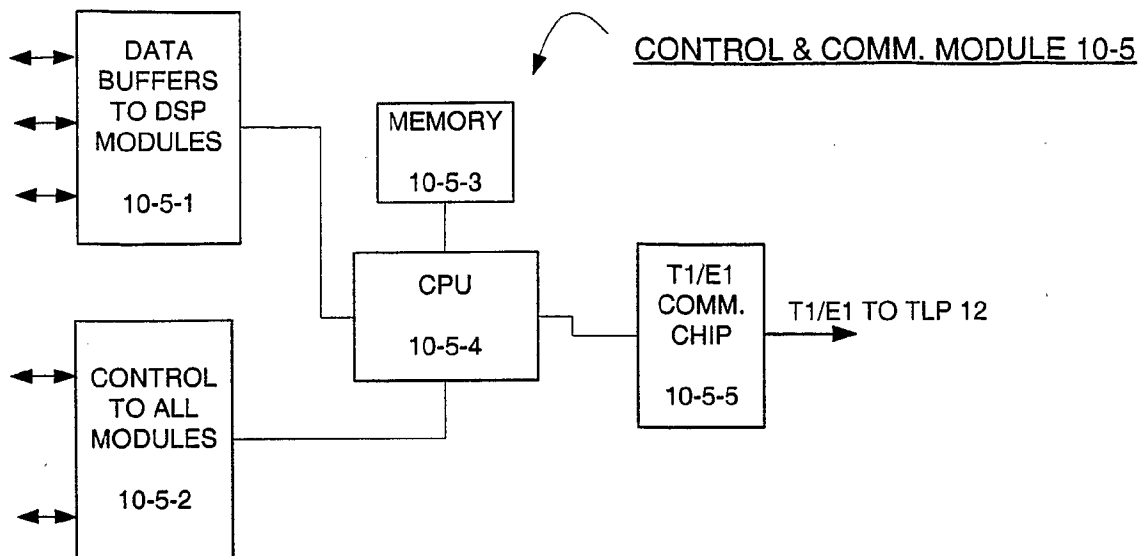


FIGURE 2F

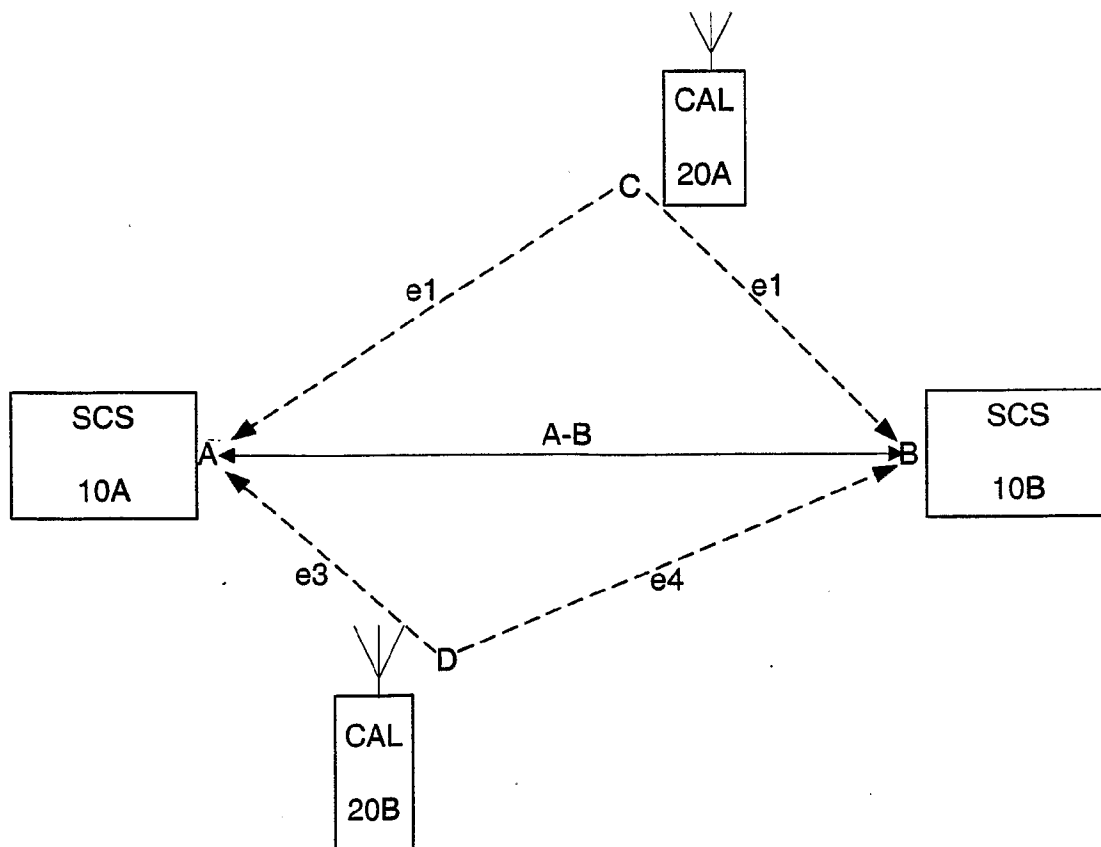


FIGURE 2G

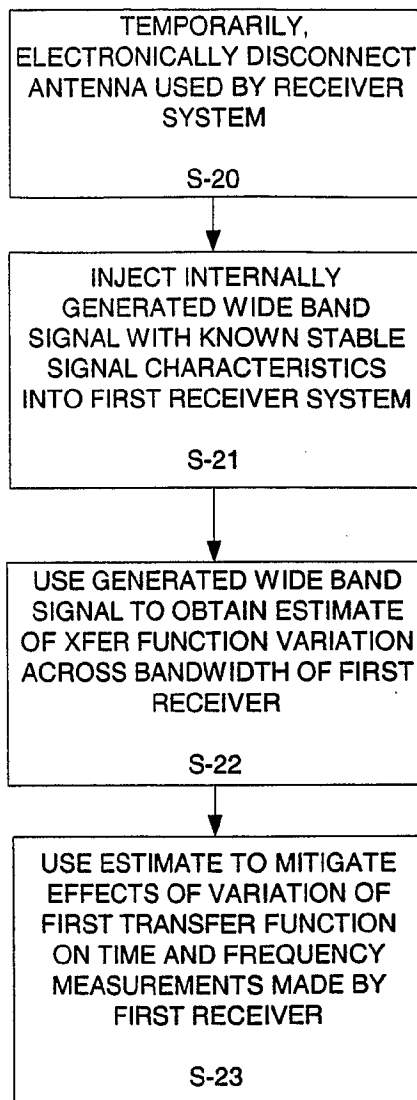


FIGURE 2H

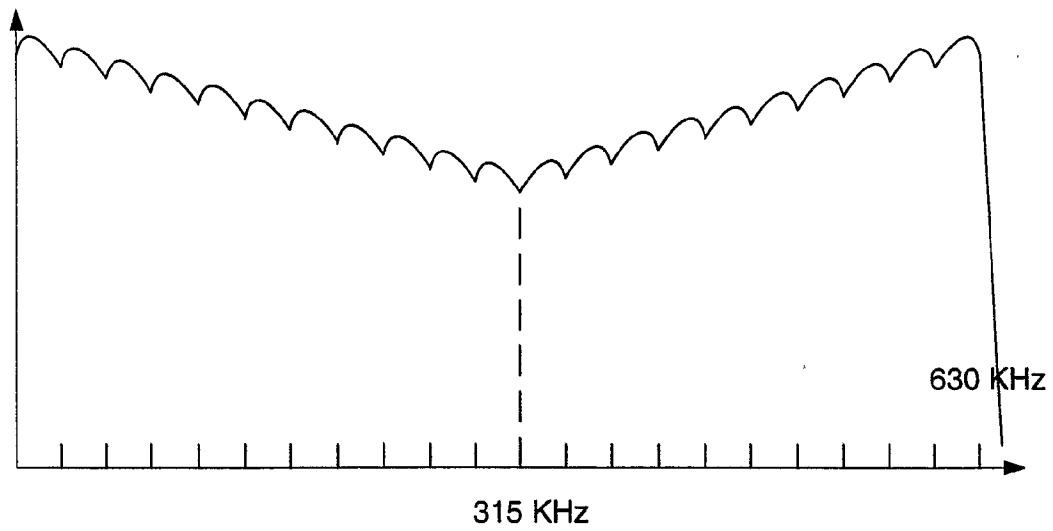


FIGURE 2I

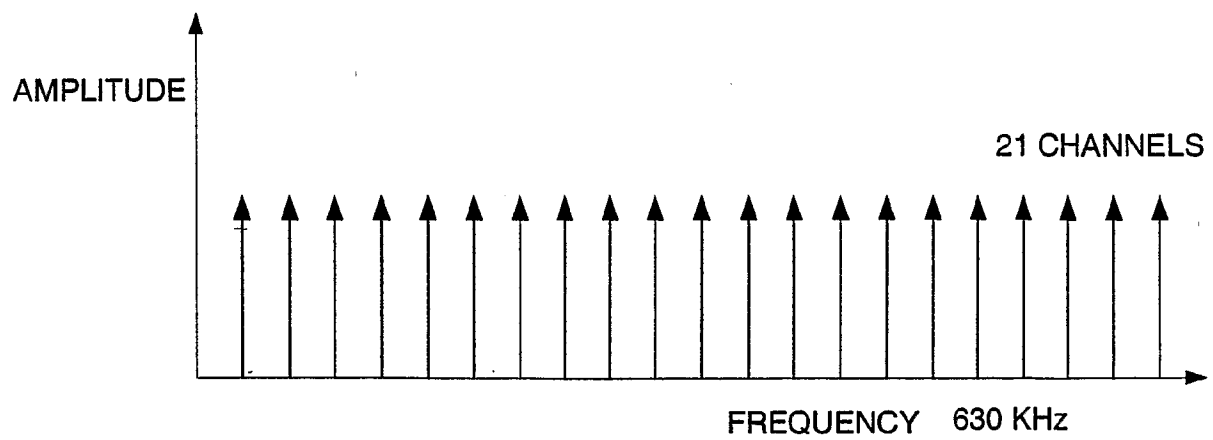


FIGURE 2J

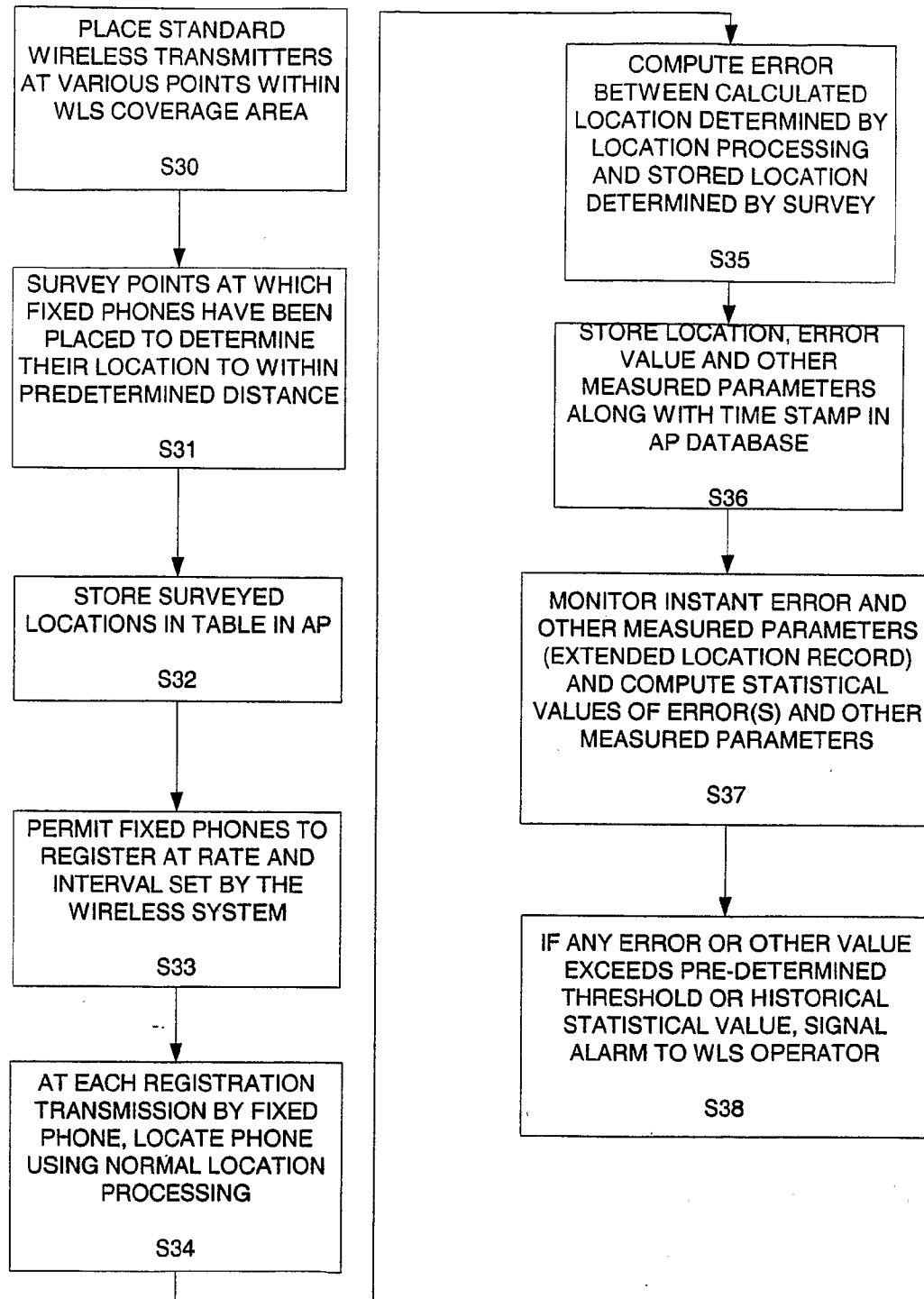


FIGURE 2K

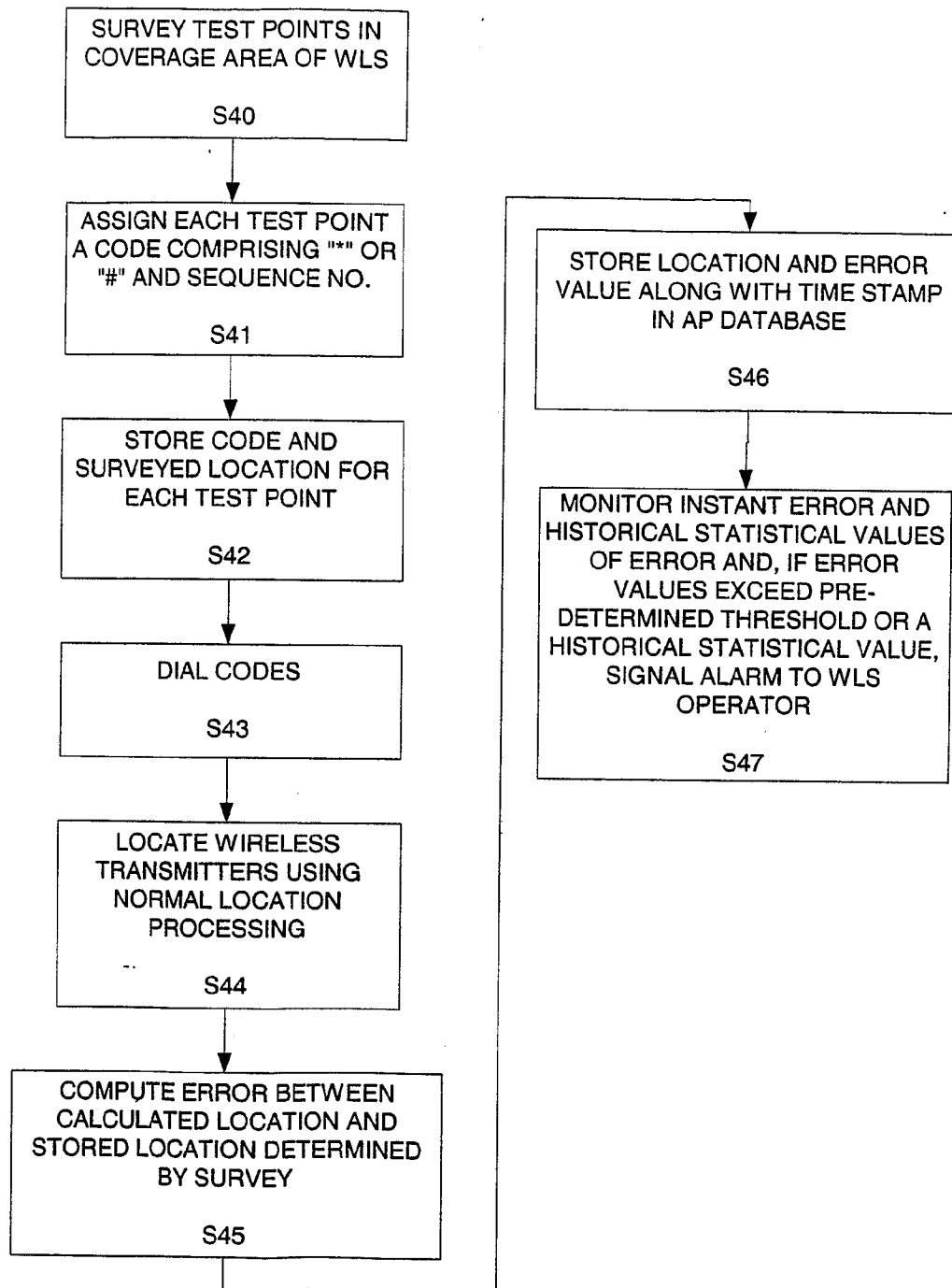


FIGURE 2L

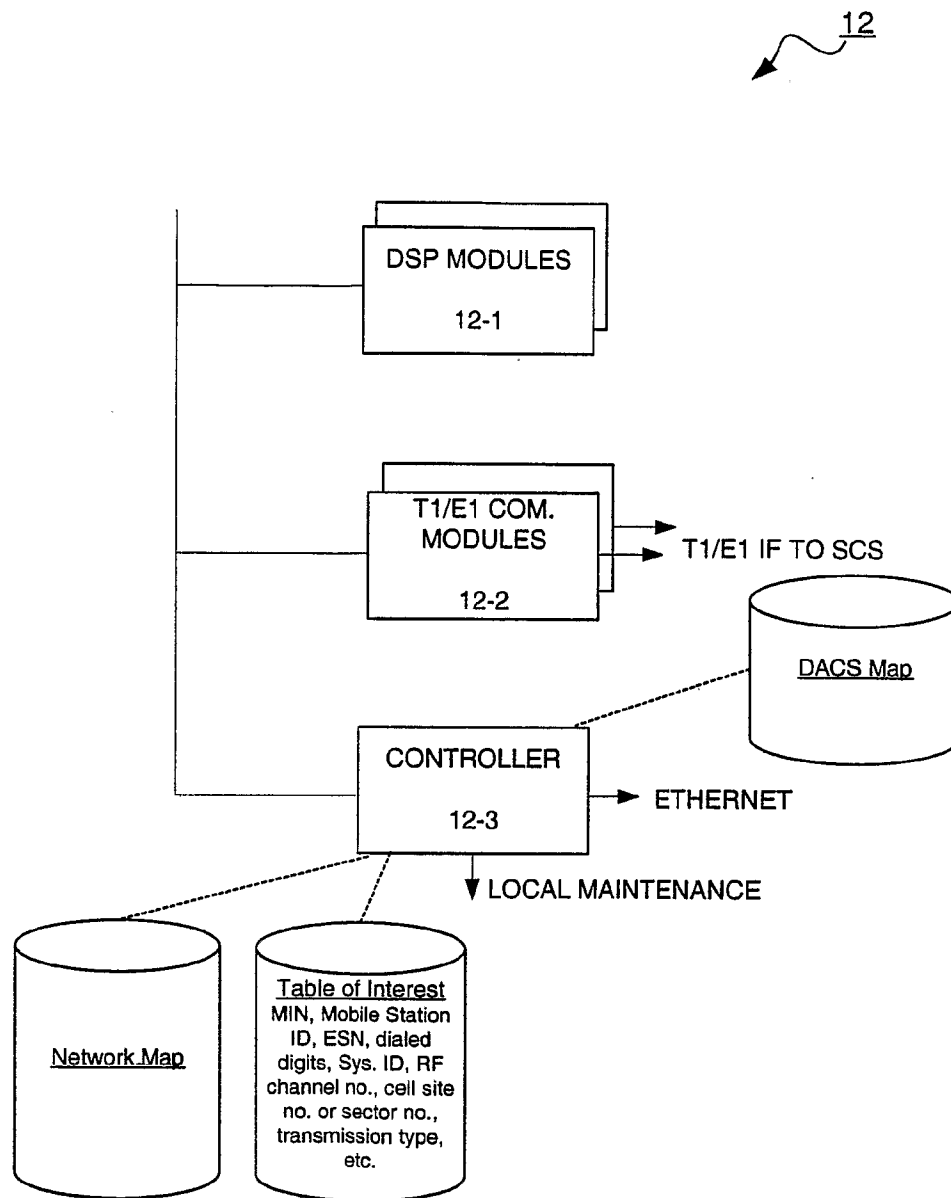


FIGURE 3

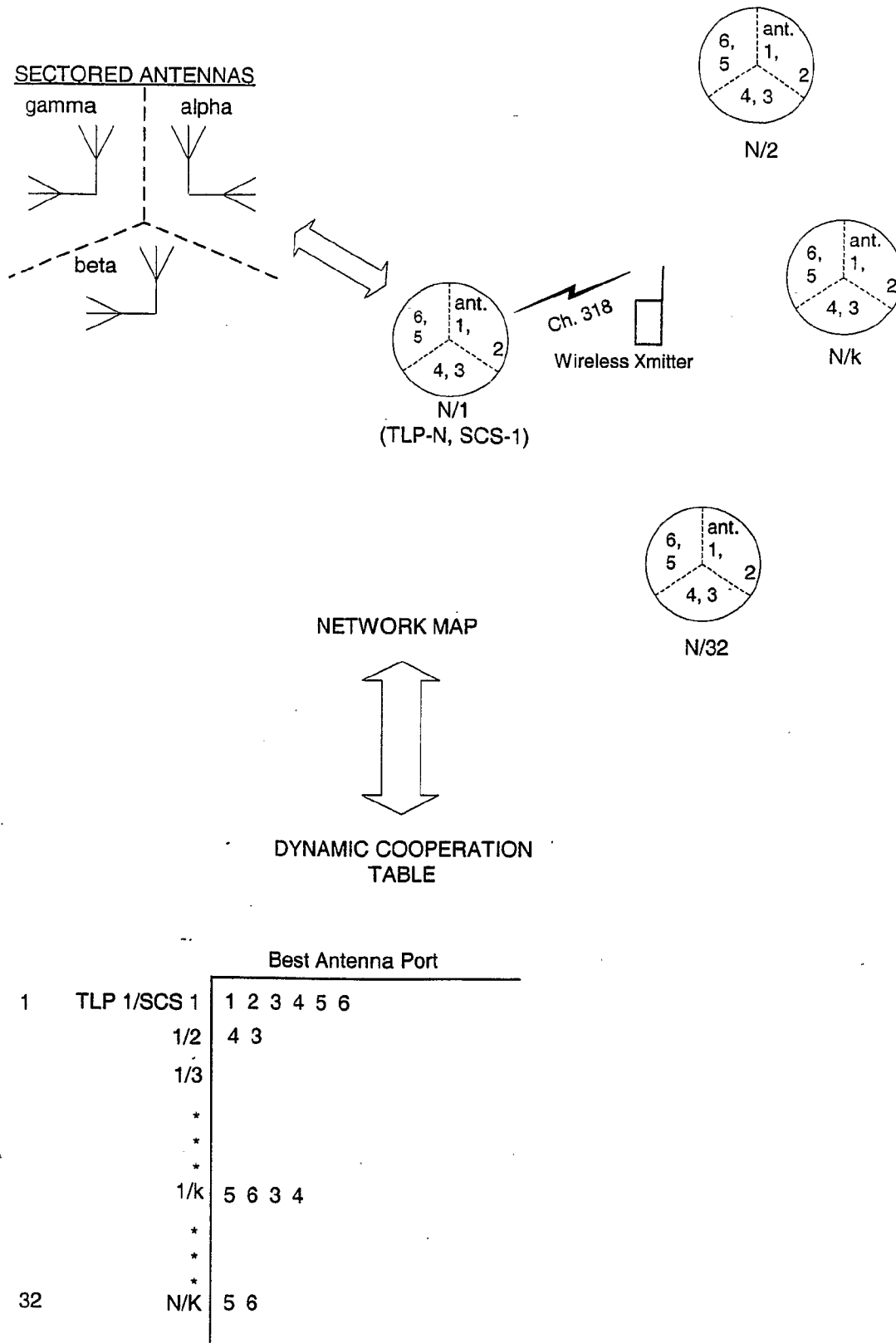


FIGURE 3A

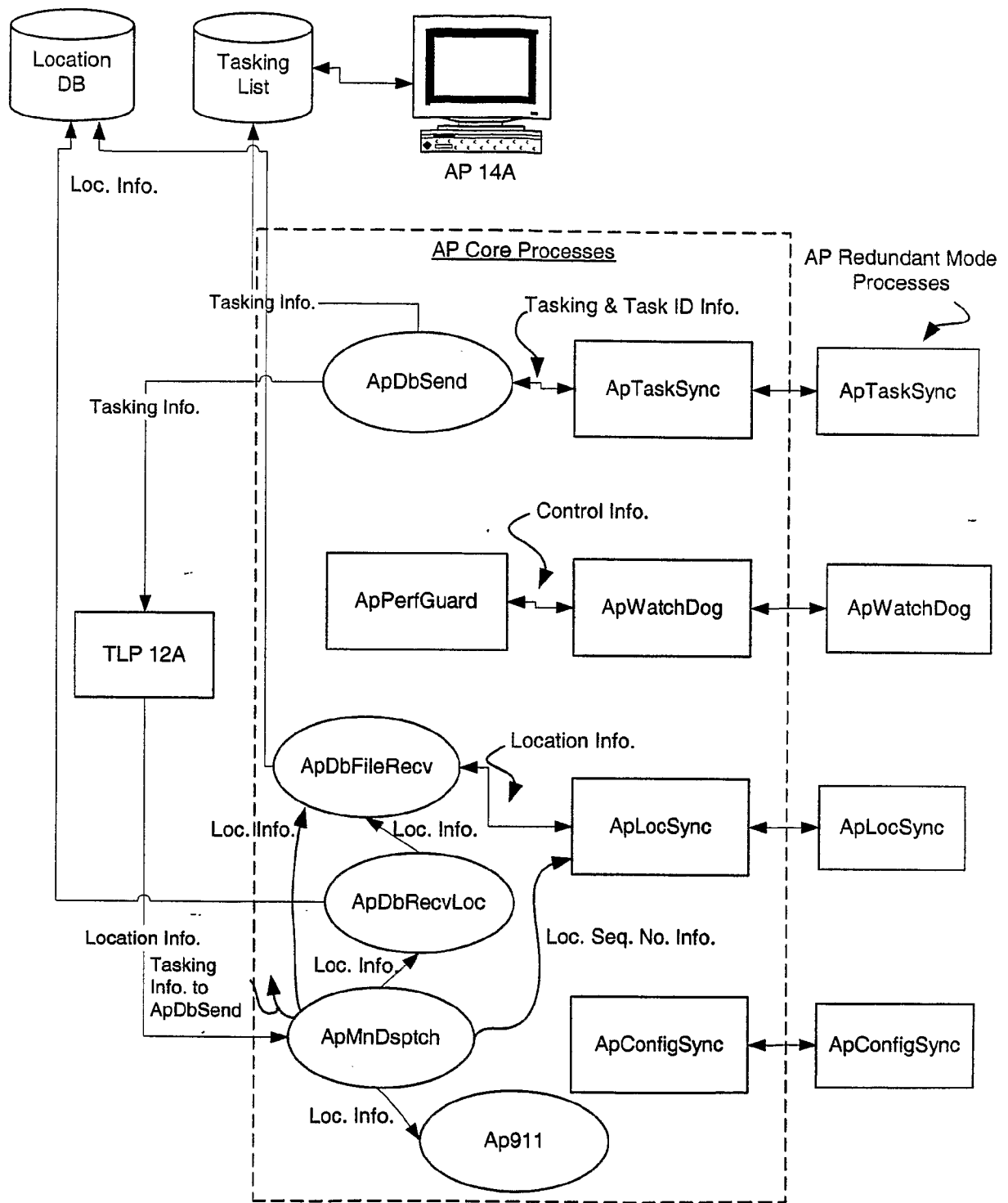


FIGURE 4

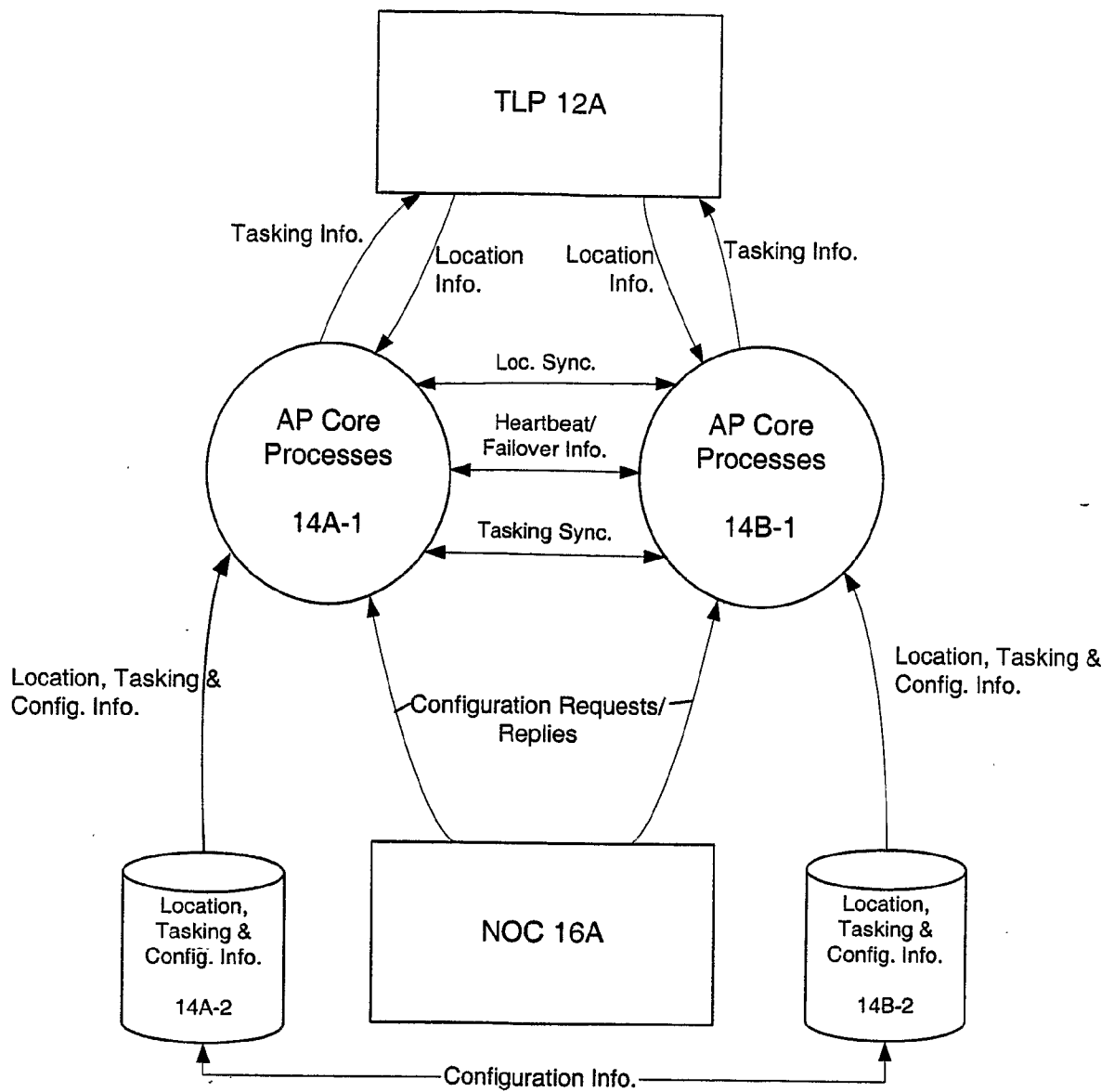


FIGURE 4A

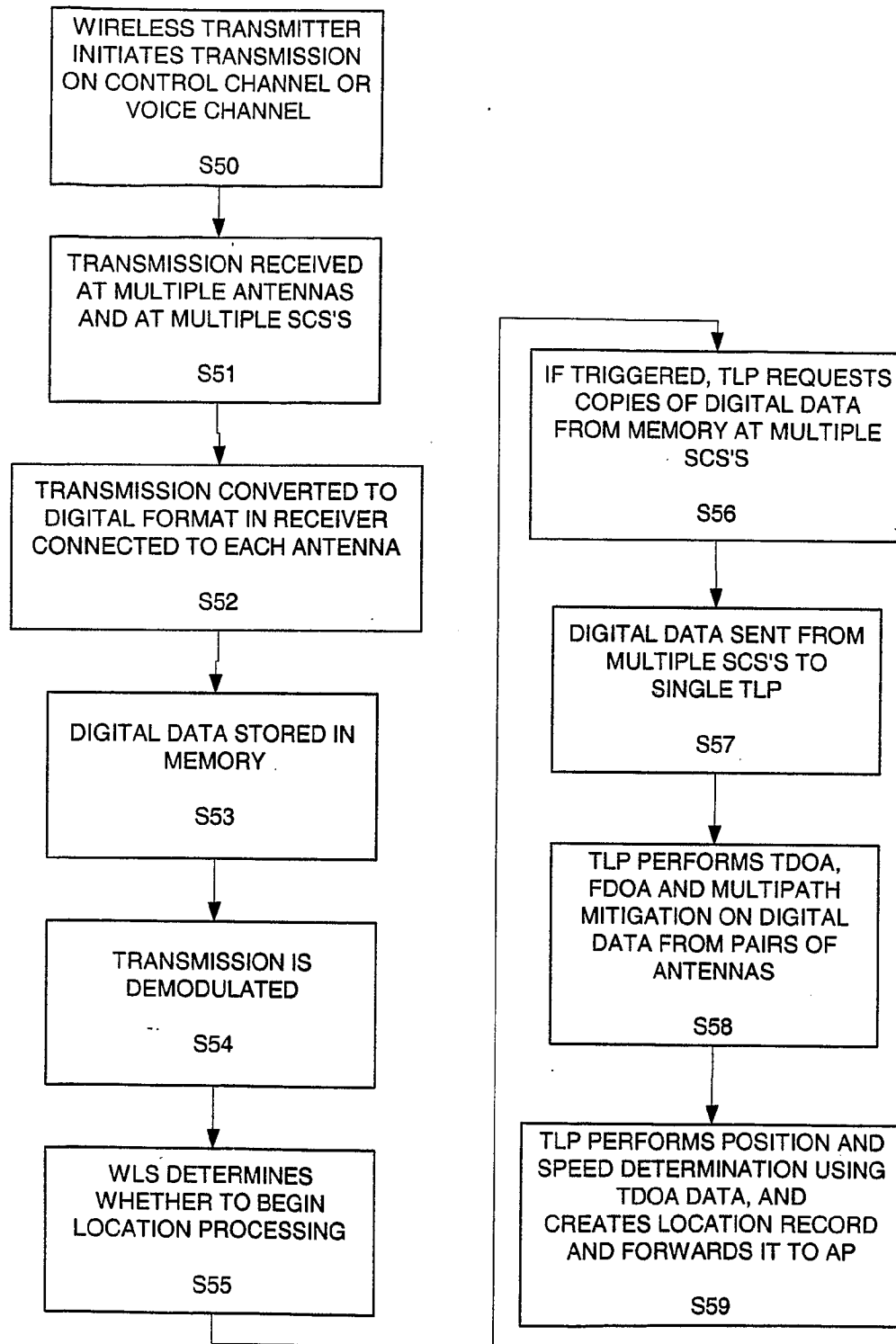


FIGURE 5

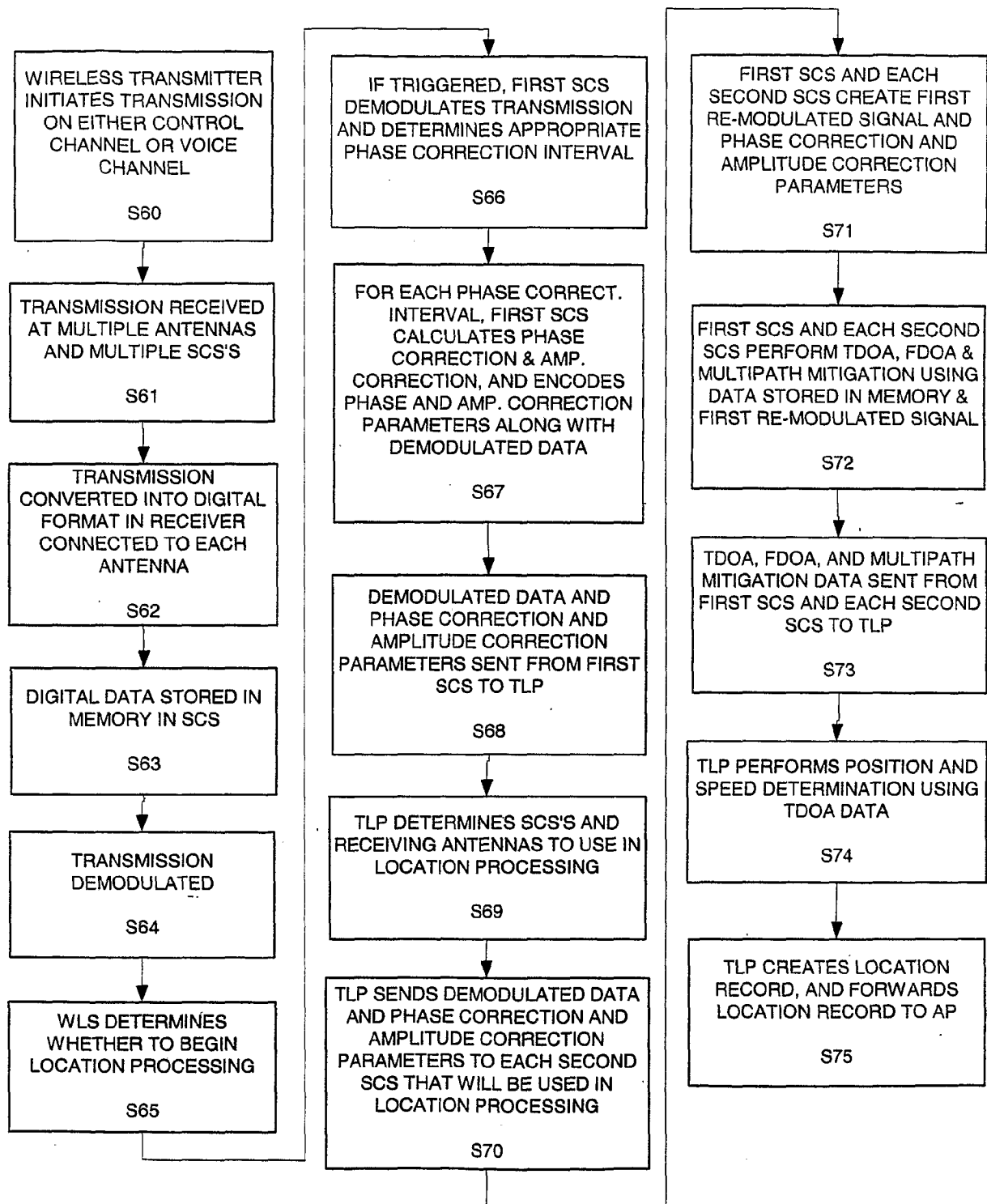


FIGURE 6

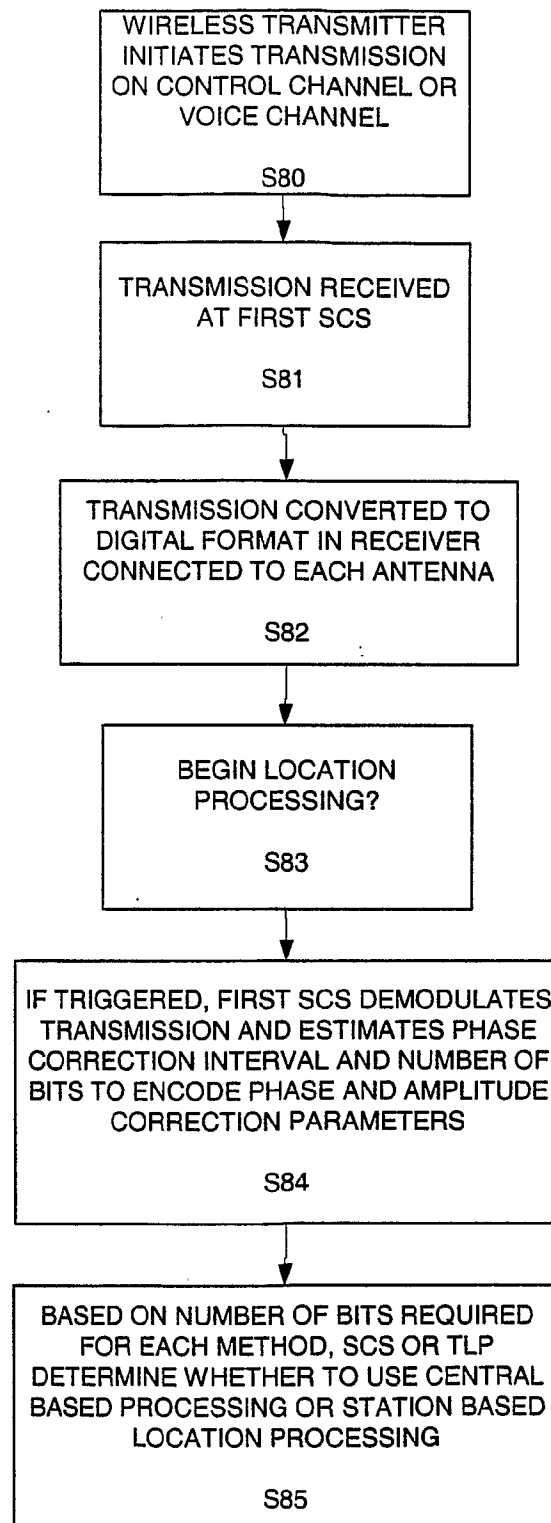


FIGURE 7

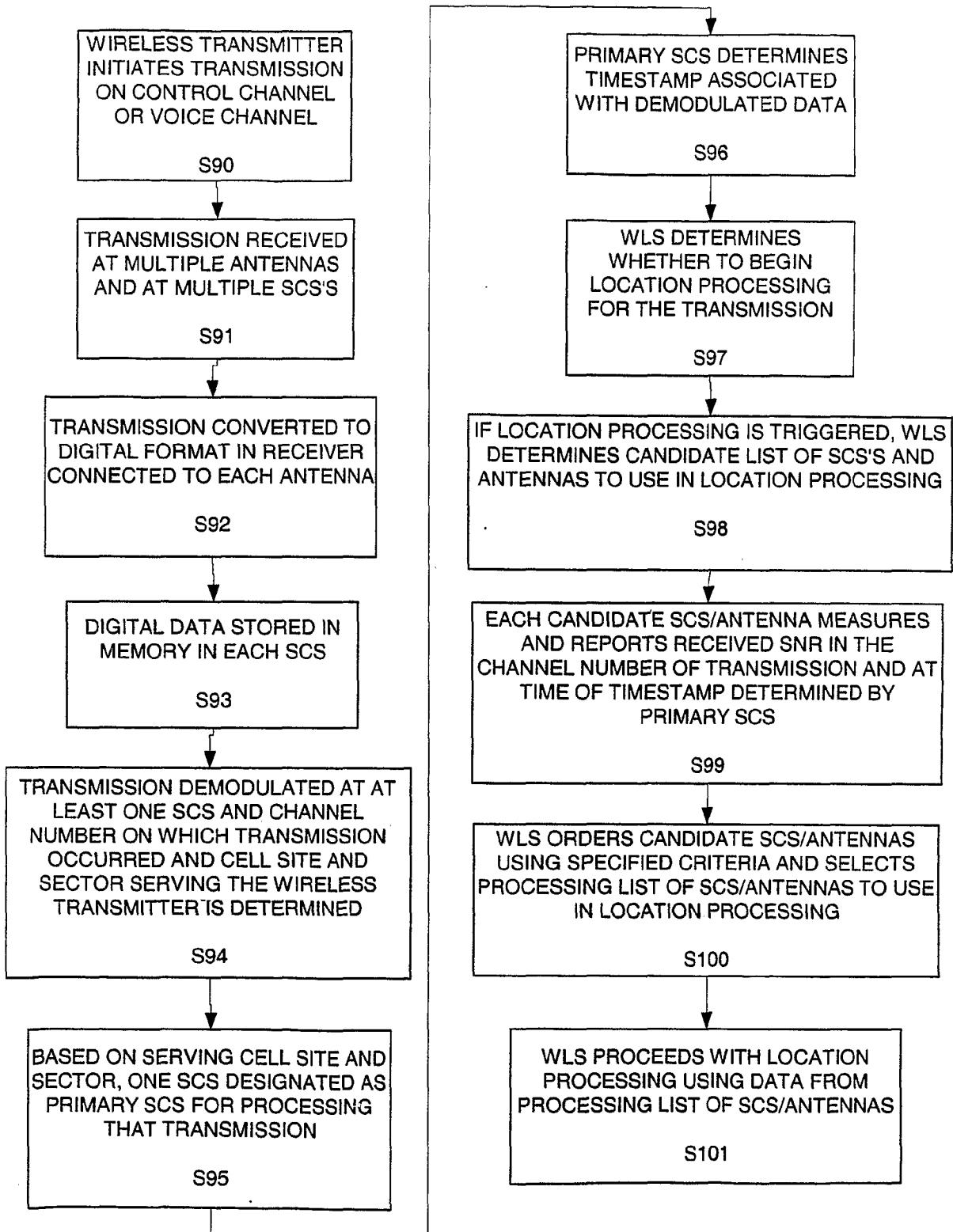


FIGURE 8

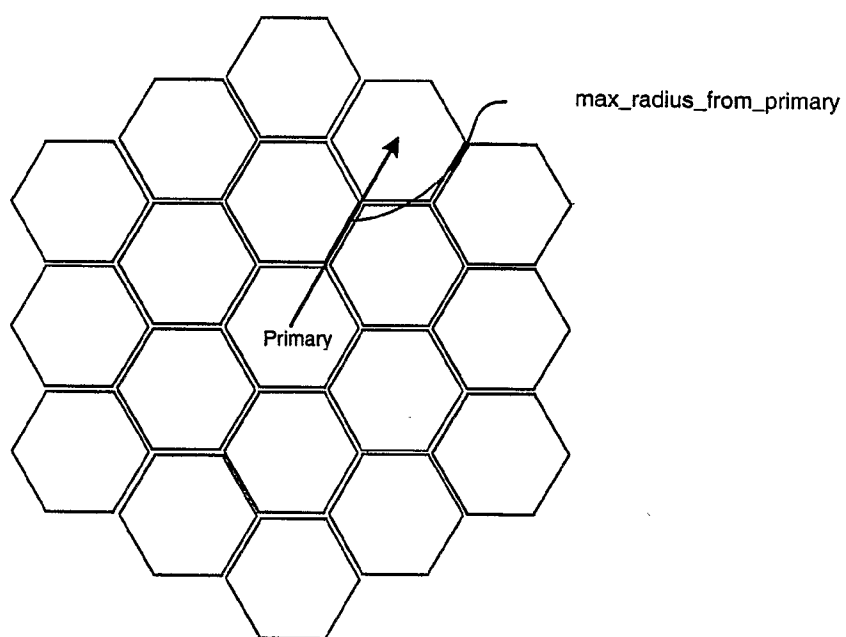


FIGURE 9

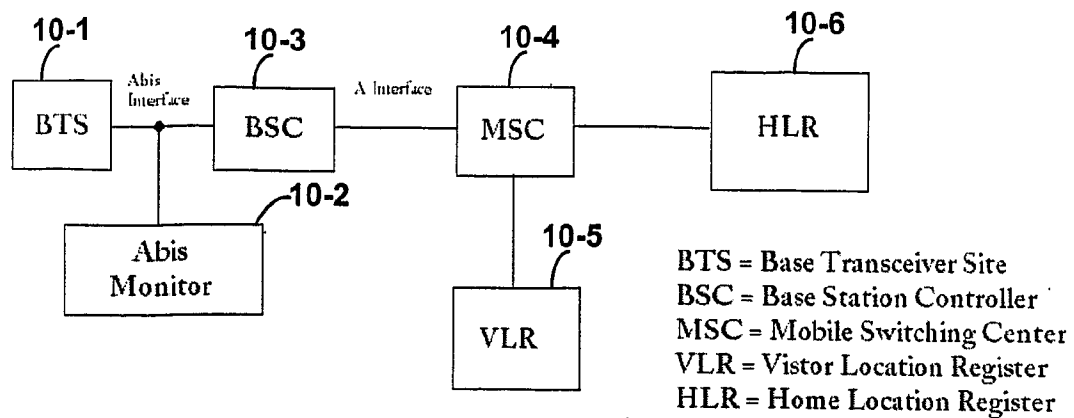


FIGURE 10

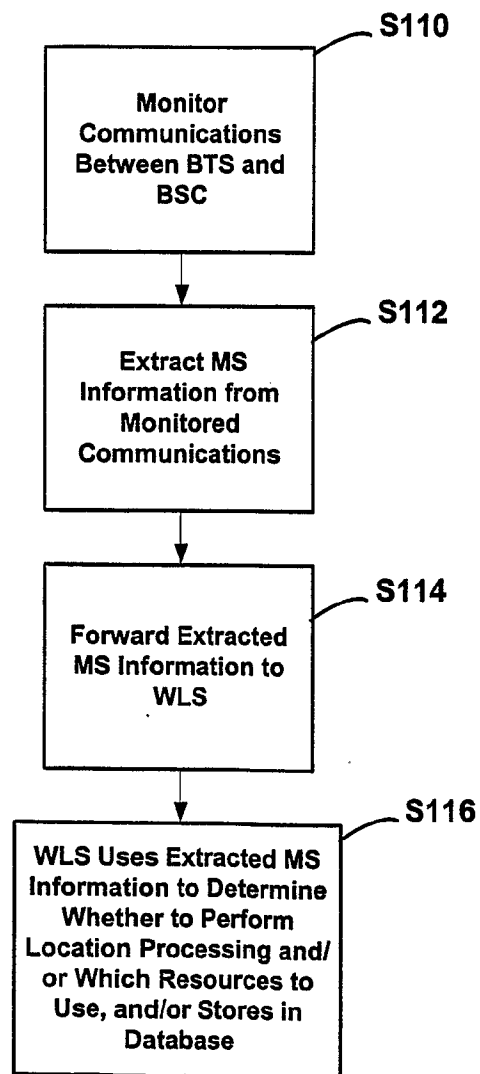


FIGURE 11



FIGURE 12A (CALL SETUP FOR MS-ORIGINATING CALL)



FIGURE 12B

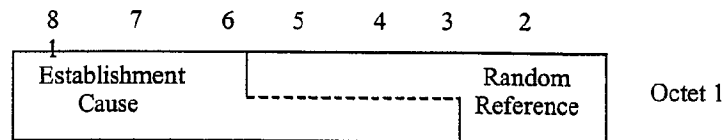


FIGURE 12C

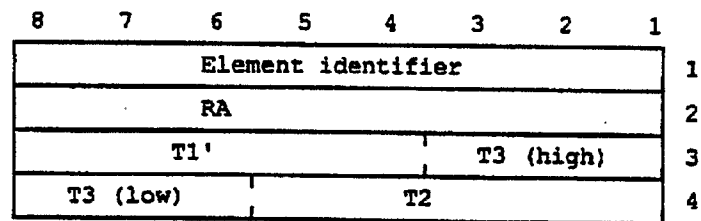


FIGURE 12D

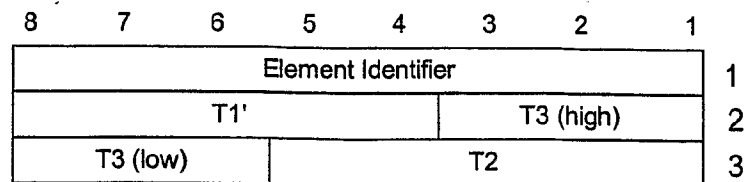


FIGURE 12E

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Full Imma. Assign Info	9.3.35	M	TLV	25

FIGURE 12F

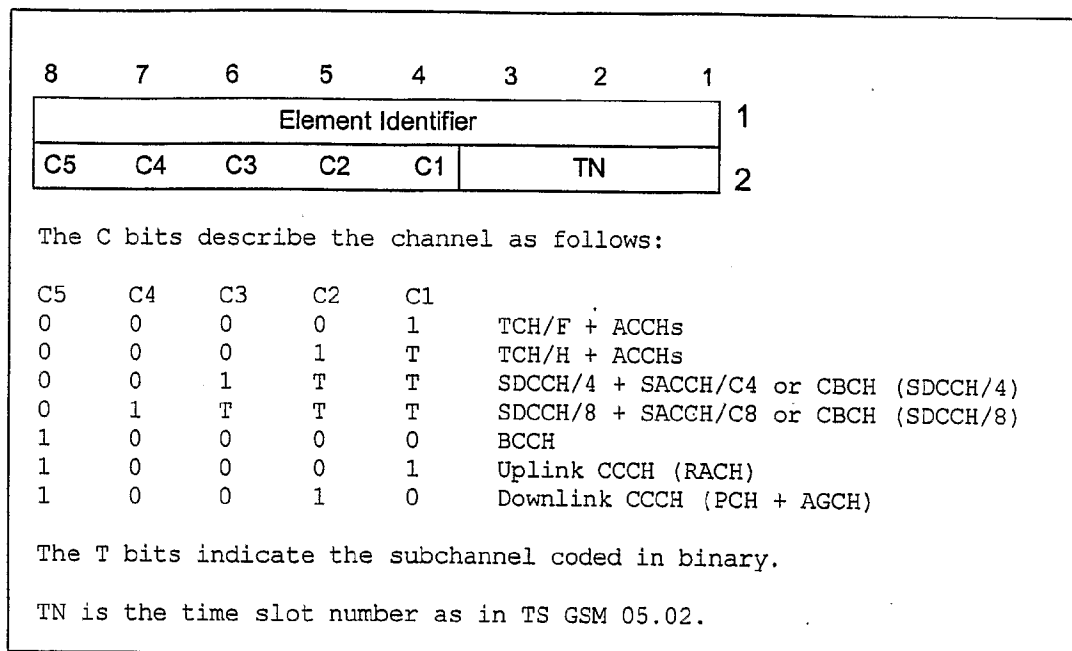


FIGURE 12G

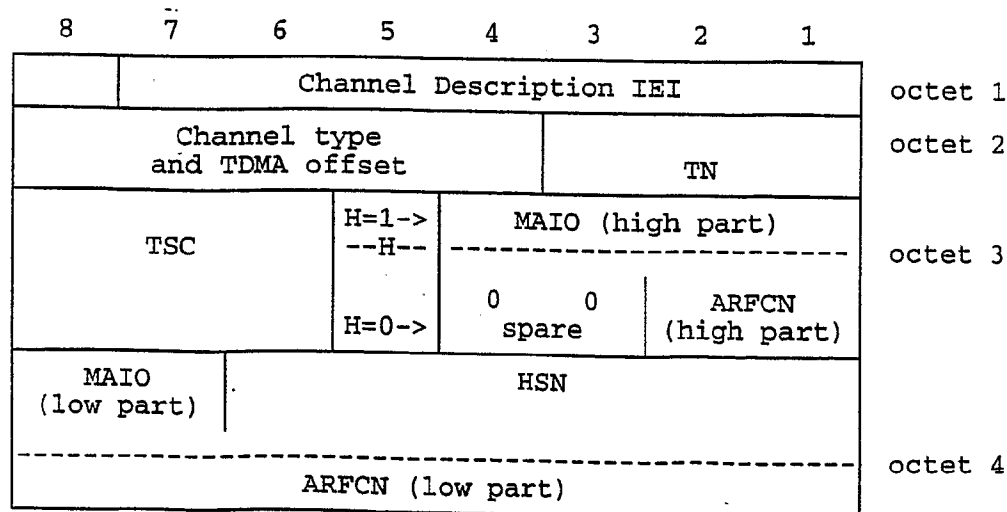
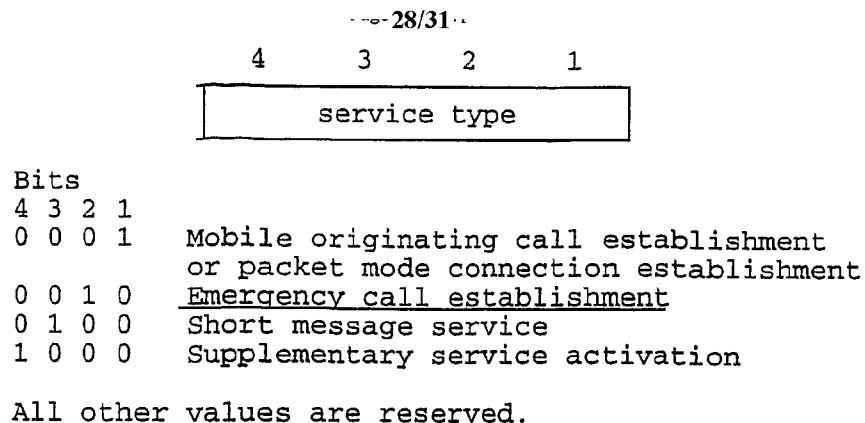


FIGURE 12H

**FIGURE 12I (BIT PATTERNS IN CM SERVICE TYPES)**

8	7	6	5	4	3	2	1		
		Mobile Station Classmark 2 IEI						octet 1	
Length of mobile station classmark 2 contents								octet 2	
0 spare		Revision level		0 spare		A5/1		RF power capability	octet 3
0 spare		0 spare		SS Screen. Indicator		SM ca pabi.		0 0 0 spare	octet 4
CM3		0 0 0 0 0 spare				A5/3		A5/2	octet 5

FIGURE 12J (MS CLASSMARK FIELDS IN CM SERVICE REQ.)

8	7	6	5	4	3	2	1	
Mobile Identity IEI								octet 1
Length of mobile identity contents								octet 2
Identity digit 1				odd/ even indic	Type of identity			octet 3
Identity digit p+1				Identity digit p				octet 4*

FIGURE 12K (FORMAT OF MOBILE ID FIELDS)

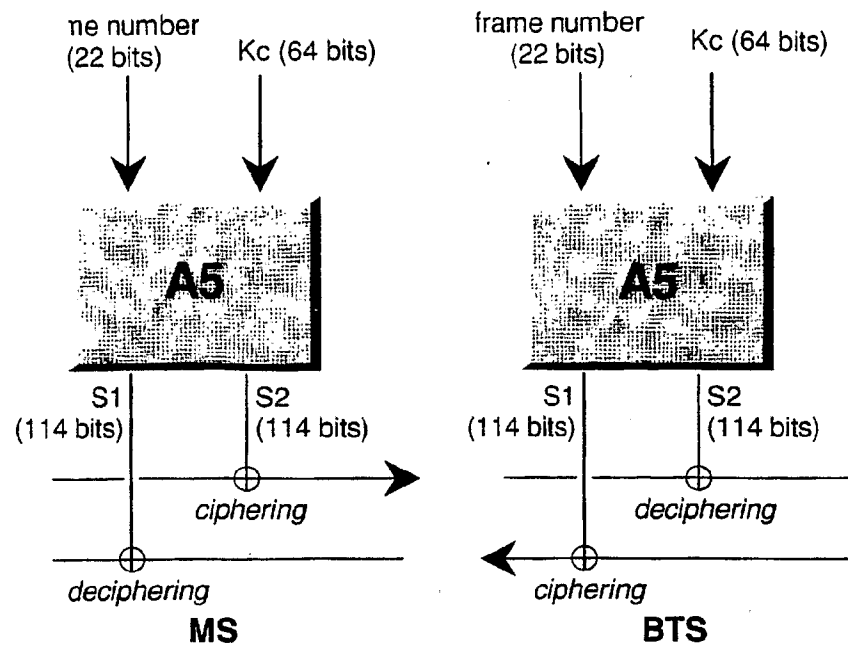


FIGURE 12L

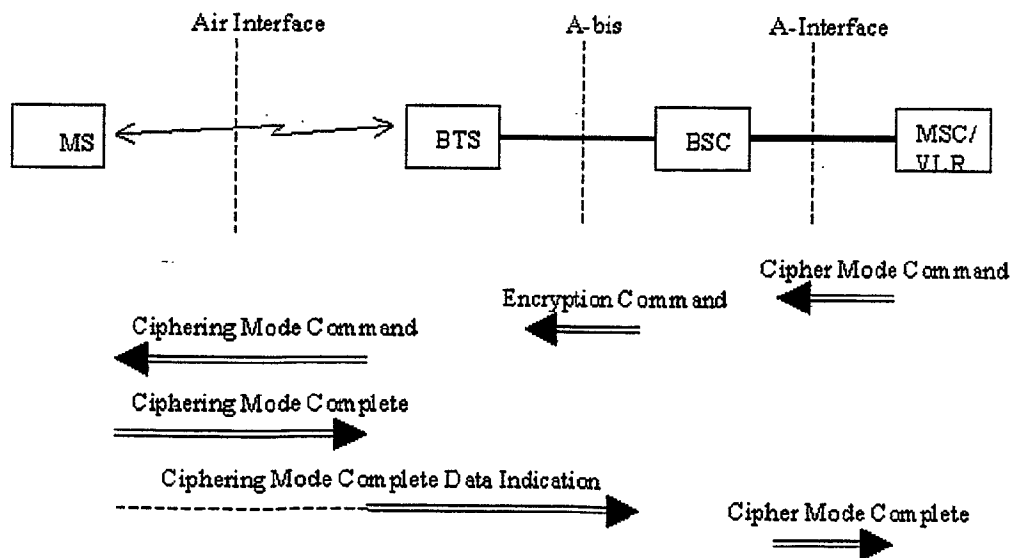


FIGURE 12M

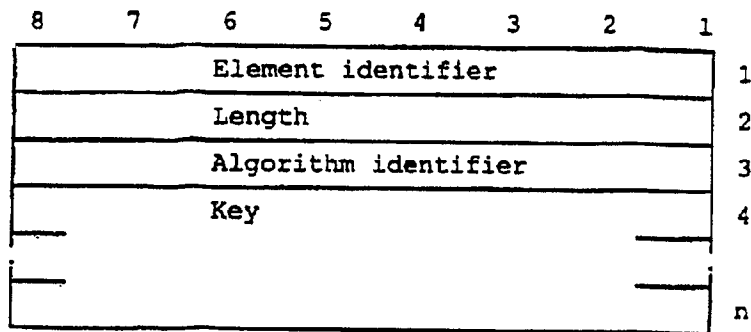


FIGURE 12N

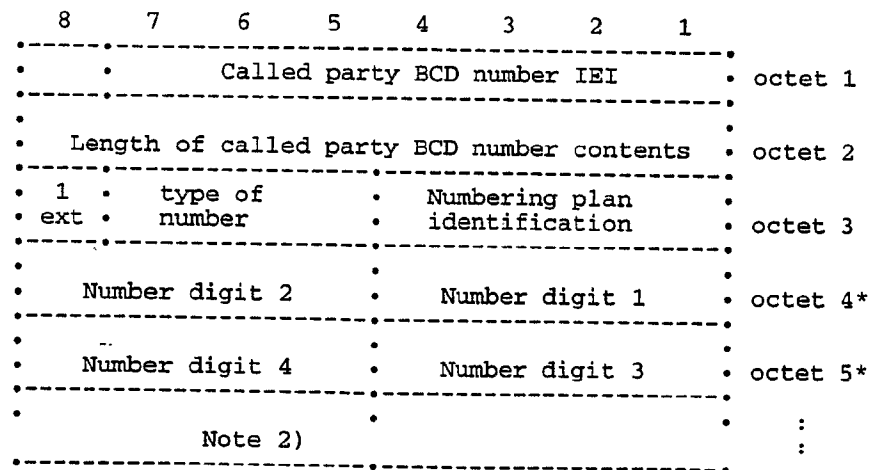


FIGURE 12O

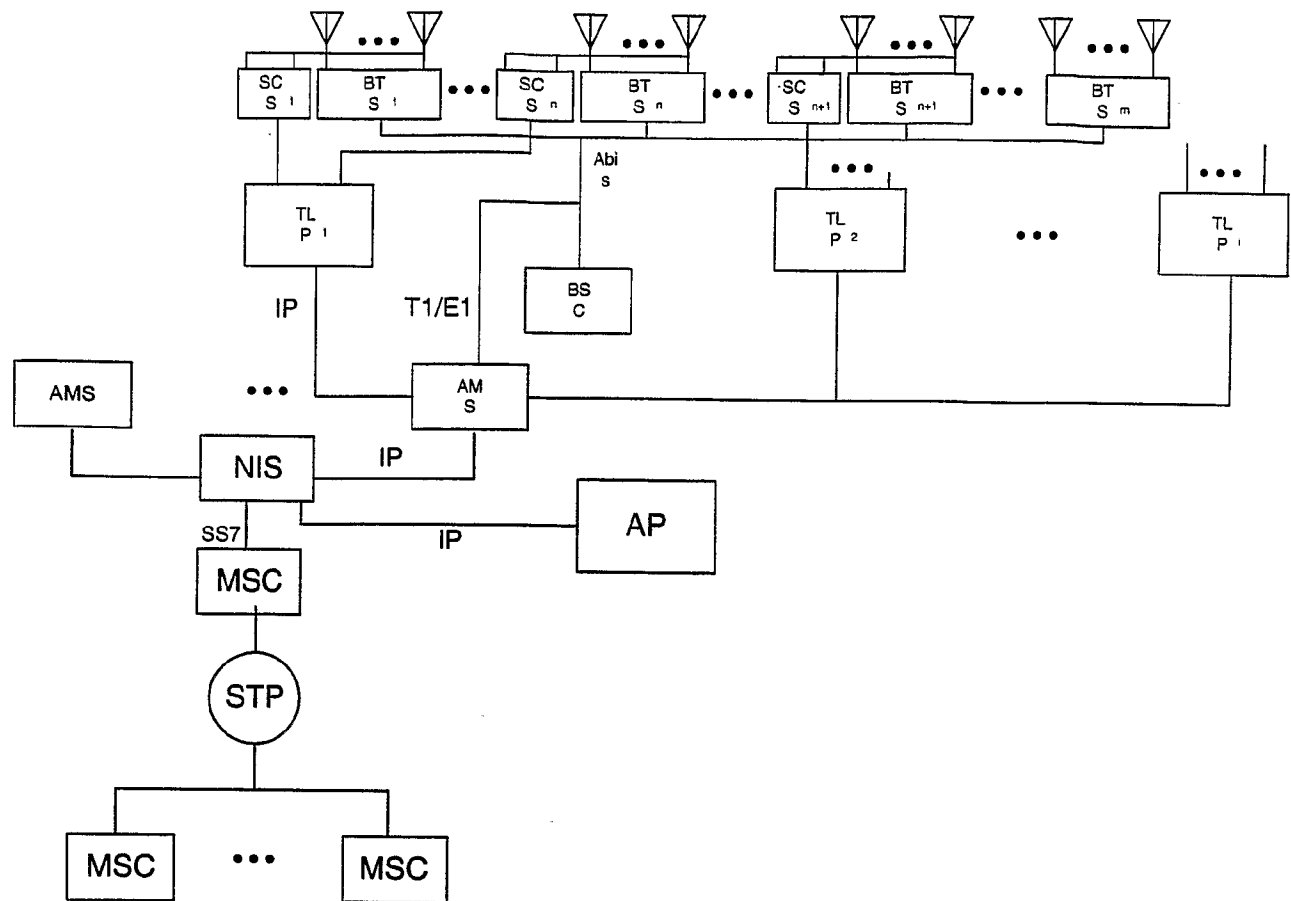


FIGURE 12P

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/22390

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20
US CL : 455/456, 560

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 455/456, 560, 561, 422; 370/310, 328

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,061,565 A (INNES et al.) 09 May 2000 (09.05.2000), columns 3-5.	1, 4-6, 14, 24
---		-----
Y		2-3, 7-13, 15-23, 25-33
Y	US 5,884,175 A (SCHIEFER et al.) 16 March 1999 (16.03.1999), column 19 lines 3-30.	2-3, 7-13, 15-23, 25-33
A,E	US 6,430,397 B1 (WILLRETT) 06 August 2002 (06.08.2002), columns 2-3.	1-33
A	US 6,088,587 A (ABBADESSA) 11 July 2000 (11.07.2000), columns 5-6, column 8 lines 38-67, column 14 lines 30-67, column 15 line 59 to column 16 line 8.	1-33

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"B" earlier application or patent published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search

04 December 2002 (04.12.2002)

Date of mailing of the international search report

19 DEC 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Nguyen T V

Telephone No. (703) 305-3900

CORRECTED VERSION

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
30 January 2003 (30.01.2003)

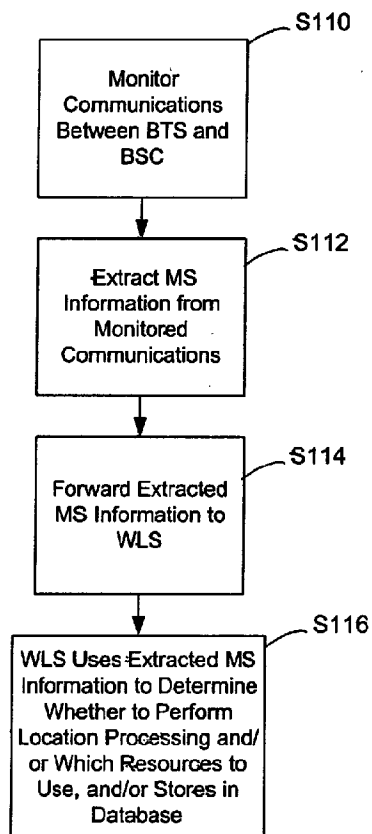
PCT

(10) International Publication Number
WO 2003/009612 A1

- (51) International Patent Classification⁷: **H04Q 7/20**
- (21) International Application Number:
PCT/US2002/022390
- (22) International Filing Date: 15 July 2002 (15.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/909,221 18 July 2001 (18.07.2001) US
- (71) Applicant (for all designated States except US): **TRUE-POSITION, INC.** [US/US]; 780 Fifth Avenue, King of Prussia, PA 19406 (US).
- (72) Inventor; and
(75) Inventor/Applicant (for US only): **ANDERSON, Robert, J.** [US/US]; 704 Deer Run, Norristown, PA 19403 (US).
- (74) Agent: **STEIN, Michael, D.**; Woodcock Washburn LLP, 46th Floor, One Liberty Place, Philadelphia, PA 19103 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: MONITORING OF CALL INFORMATION IN A WIRELESS LOCATION SYSTEM



(57) Abstract: In an overlay Wireless Location System, an Abis interface is monitored to obtain information used to locate GSM phones (S116). Signaling links of the Abis interface are passively monitored to obtain certain information, such as control and traffic channel assignment, called number, and mobile identification, which is not available from the GSM air interface of the reverse channel (S110-S116). This approach also applies to IDEN and can be broadened to include CDMA systems where the GSM architecture has been used and the system includes a separated BTS to BSC interface.

WO 2003/009612 A1



(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(48) Date of publication of this corrected version:

29 April 2004

(15) Information about Correction:

see PCT Gazette No. 18/2004 of 29 April 2004, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

MONITORING OF CALL INFORMATION IN A WIRELESS LOCATION SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

5 This is a continuation-in-part of U.S. Patent Application Serial No. 09/539,352, filed March 31, 2000, "Centralized Database for a Wireless Location System," which is a continuation of U.S. Patent Application Serial No. 09/227,764, filed January 8, 1999, now U.S. Patent No. 6,184,829 B1, Feb. 6, 2001, "Calibration for Wireless Location System."

10

FIELD OF THE INVENTION

 The present invention relates generally to methods and apparatus for locating wireless transmitters, such as those used in analog or digital cellular systems, personal communications systems (PCS), enhanced specialized mobile radios (ESMRs), and other
15 types of wireless communications systems. More particularly, the present invention relates to the collection of call information from the wireless network's non-air interfaces to facilitate location via TDOA, AOA, and/or TDOA/AOA hybrid wireless location systems in wireless systems having a separated Base Transceiver Station (BTS) and Base Station Controller (BSC).

20

BACKGROUND OF THE INVENTION

 Early work relating to Wireless Location Systems is described in U.S. Patent Number 5,327,144, July 5, 1994, "Cellular Telephone Location System," which discloses a system for locating cellular telephones using novel time difference of arrival (TDOA)
25 techniques. Further enhancements of the system disclosed in the '144 patent are disclosed in U.S. Patent Number 5,608,410, March 4, 1997, "System for Locating a Source of Bursty Transmissions." Both of these patents are assigned to TruePosition, Inc., the assignee of the present invention, and both are incorporated herein by reference. TruePosition has continued to develop significant enhancements to the original inventive
30 concepts and have developed techniques to further improve the accuracy of Wireless Location Systems while significantly reducing the cost of these systems. Patents relating to such enhancements include, but are not necessarily limited to: U.S. Patent No.

6,091,362, July 18, 2000, "Bandwidth Synthesis for Wireless Location System"; U.S. Patent No. 6,097,336, August 1, 2000, "Method for Improving the Accuracy of a Wireless Location System"; U.S. Patent No. 6,115,599, September 5, 2000, "Directed Retry Method for Use in a Wireless Location System"; U.S. Patent No. 6,172,644 B1, 5 January 9, 2001, "Emergency Location Method for a Wireless Location System"; and U.S. Patent No. 6,184,829 B1, February 6, 2001, "Calibration for Wireless Location System."

Over the past few years, the cellular industry has increased the number of air interface 10 protocols available for use by wireless telephones, increased the number of frequency bands in which wireless or mobile telephones may operate, and has expanded the number of terms that refer or relate to mobile telephones to include "personal communications services", "wireless", and others. The air interface protocols now include AMPS, N-AMPS, TDMA, CDMA, GSM, TACS, ESMR, GPRS, EDGE, and others. The changes 15 in terminology and increases in the number of air interfaces do not change the basic principles and inventions discovered and enhanced by the inventors. However, in keeping with the current terminology of the industry, the inventors now call the system described herein a *Wireless Location System*.

20 The inventors have conducted extensive experiments with the Wireless Location System technology to demonstrate both the viability and value of the technology. For example, several experiments were conducted during several months of 1995 and 1996 in the cities of Philadelphia and Baltimore to verify the system's ability to mitigate multipath in large urban environments. Then, in 1996 the inventors constructed a system in Houston that 25 was used to test the technology's effectiveness in that area and its ability to interface directly with E9-1-1 systems. Then, in 1997, the system was tested in a 350 square mile area in New Jersey and was used to locate real 9-1-1 calls from real people in trouble. Since that time, the system test has been expanded to include 125 cell sites covering an area of over 2,000 square miles. During all of these tests, techniques discussed and 30 disclosed herein were tested for effectiveness and further developed, and the system has been demonstrated to overcome the limitations of other approaches that have been proposed for locating wireless telephones.

The value and importance of the Wireless Location System has been acknowledged by the wireless communications industry. In June 1996, the Federal Communications Commission issued requirements for the wireless communications industry to deploy
5 location systems for use in locating wireless 9-1-1 callers, with a deadline of October 2001. The location of wireless E9-1-1 callers will save response time, save lives, and save enormous costs because of reduced use of emergency responses resources. In addition, numerous surveys and studies have concluded that various wireless applications, such as location sensitive billing, fleet management, and others, will have
10 great commercial values in the coming years.

Background on Wireless Communications Systems

There are many different types of air interface protocols used for wireless communications systems. These protocols are used in different frequency bands, both in
15 the U.S. and internationally. The frequency band does not impact the Wireless Location System's effectiveness at locating wireless telephones.

All air interface protocols use two types of "channels". The first type includes control channels that are used for conveying information about the wireless telephone or
20 transmitter, for initiating or terminating calls, or for transferring bursty data. For example, some types of short messaging services transfer data over the control channel. In different air interfaces, control channels are known by different terminology, but the use of the control channels in each air interface is similar. Control channels generally have identifying information about the wireless telephone or transmitter contained in the
25 transmission. Control channels also include various data transfer protocols that are not voice specific – these include General Packet Radio Service (GPRS), Enhanced Data rate for GSM Evolution (EDGE), and Enhanced GPRS (EGPRS).

The second type includes voice channels that are typically used for conveying voice
30 communications over the air interface. These channels are only used after a call has been set up using the control channels. Voice channels will typically use dedicated resources within the wireless communications system whereas control channels will use shared

resources. This distinction will generally make the use of control channels for wireless location purposes more cost effective than the use of voice channels, although there are some applications for which regular location on the voice channel is desired. Voice channels generally do not have identifying information about the wireless telephone or transmitter in the transmission. Some of the differences in the air interface protocols are discussed below:

AMPS – This is the original air interface protocol used for cellular communications in the U.S. In the AMPS system, separate dedicated channels are assigned for use by control channels (RCC). According to the TIA/EIA Standard IS-553A, every control channel block must begin at cellular channel 333 or 334, but the block may be of variable length. In the U.S., by convention, the AMPS control channel block is 21 channels wide, but the use of a 26-channel block is also known. A reverse voice channel (RVC) may occupy any channel that is not assigned to a control channel. The control channel modulation is FSK (frequency shift keying), while the voice channels are modulated using FM (frequency modulation).

N-AMPS – This air interface is an expansion of the AMPS air interface protocol, and is defined in EIA/TIA standard IS-88. The control channels are substantially the same as for AMPS; however, the voice channels are different. The voice channels occupy less than 10 KHz of bandwidth, versus the 30 KHz used for AMPS, and the modulation is FM.

TDMA – This interface is also known D-AMPS, and is defined in EIA/TIA standard IS-136. This air interface is characterized by the use of both frequency and time separation. Control channels are known as Digital Control Channels (DCCH) and are transmitted in bursts in timeslots assigned for use by DCCH. Unlike AMPS, DCCH may be assigned anywhere in the frequency band, although there are generally some frequency assignments that are more attractive than others based upon the use of probability blocks. Voice channels are known as Digital Traffic Channels (DTC). DCCH and DTC may occupy the same frequency assignments, but not the same timeslot assignment in a given

frequency assignment. DCCH and DTC use the same modulation scheme, known as $\pi/4$ DQPSK (differential quadrature phase shift keying). In the cellular band, a carrier may use both the AMPS and TDMA protocols, as long as the frequency assignments for each protocol are kept separated. A carrier may also aggregate digital channels together to
5 support higher speed data transfer protocols such as GPRS and EDGE.

CDMA – This air interface is defined by EIA/TIA standard IS-95A. This air interface is characterized by the use of both frequency and code separation. However, because adjacent cell sites may use the same frequency sets, CDMA is also characterized by very
10 careful power control. This careful power control leads to a situation known to those skilled in the art as the near-far problem, which makes wireless location difficult for most approaches to function properly. Control channels are known as Access Channels, and voice channels are known as Traffic Channels. Access and Traffic Channels may share the same frequency band, but are separated by code. Access and Traffic Channels
15 use the same modulation scheme, known as OQPSK. CDMA can support higher speed data transfer protocols by aggregating codes together.

GSM - the international standard Global System for Mobile Communications defines this air interface. Like TDMA, GSM is characterized by the use of both frequency and time
20 separation. The channel bandwidth is 200 KHz, which is wider than the 30 KHz used for TDMA. Control channels are known as Standalone Dedicated Control Channels (SDCCH), and are transmitted in bursts in timeslots assigned for use by SDCCH. SDCCH may be assigned anywhere in the frequency band. Voice channels are known as Traffic Channels (TCH). SDCCH and TCH may occupy the same frequency
25 assignments, but not the same timeslot assignment in a given frequency assignment. SDCCH and TCH use the same modulation scheme, known as GMSK. GSM can also support higher data transfer protocols such as GPRS and EGPRS.

Within this specification the reference to any one of the air interfaces may refer to all of
30 the air interfaces, unless specified otherwise. Additionally, a reference to control channels or voice channels may refer to all types of control or voice channels, whatever

the preferred terminology for a particular air interface. Finally, there are many more types of air interfaces used throughout the world, and there is no intent to exclude any air interface from the inventive concepts described within this specification. Indeed, those skilled in the art will recognize other interfaces used elsewhere are derivatives of or
5 similar in class to those described above.

SUMMARY OF THE INVENTION

The present invention is designed to collect wireless call associated information using a non-invasive, passive collection mechanism. The invention may be used to
10 determine cell, frequency, and caller information for purposes of directing a Wireless Location System. For example, in an overlay Wireless Location System, an Abis interface may be monitored to obtain information used to locate GSM phones. In this implementation, signaling links of the Abis interface are passively monitored to obtain certain information, such as control and traffic channel assignment, called number, and
15 mobile identification, which is not available from the GSM air interface of the reverse channel. This approach also applies to IDEN and can be broadened to include CDMA systems where the GSM architecture has been used and the system includes a separate BTS to BSC interface.

20 Other features and advantages of the invention are disclosed below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figures 1 and 1A schematically depict a Wireless Location System in accordance with the present invention.

25

Figure 2 schematically depicts a Signal Collection System (SCS) 10 in accordance with the present invention.

Figure 2A schematically depicts a receiver module 10-2 employed by the Signal
30 Collection System.

Figures 2B and 2C schematically depict alternative ways of coupling the receiver module(s) 10-2 to the antennas 10-1.

Figure 2C-1 is a flowchart of a process employed by the Wireless Location System when
5 using narrowband receiver modules.

Figure 2D schematically depicts a DSP module 10-3 employed in the Signal Collection System in accordance with the present invention.

10 Figure 2E is a flowchart of the operation of the DSP module(s) 10-3, and Figure 2E-1 is a flowchart of the process employed by the DSP modules for detecting active channels.

Figure 2F schematically depicts a Control and Communications Module 10-5 in accordance with the present invention.

15

Figures 2G-2J depict aspects of the presently preferred SCS calibration methods. Figure 2G is a schematic illustration of baselines and error values used to explain an external calibration method in accordance with the present invention. Figure 2H is a flowchart of an internal calibration method. Figure 2I is an exemplary transfer function of an AMPS
20 control channel and Figure 2J depicts an exemplary comb signal.

Figures 2K and 2L are flowcharts of two methods for monitoring performance of a Wireless Location System in accordance with the present invention.

25 Figure 3 schematically depicts a TDOA Location Processor 12 in accordance with the present invention.

Figure 3A depicts the structure of an exemplary network map maintained by the TLP controllers in accordance with the present invention.

30

Figures 4 and 4A schematically depict different aspects of an Applications Processor 14 in accordance with the present invention.

Figure 5 is a flowchart of a central station-based location processing method in accordance with the present invention.

- 5 Figure 6 is a flowchart of a station-based location processing method in accordance with the present invention.

Figure 7 is a flowchart of a method for determining, for each transmission for which a location is desired, whether to employ central or station-based processing.

10

Figure 8 is a flowchart of a dynamic process used to select cooperating antennas and SCS's 10 used in location processing.

- 15 Figure 9 is diagram that is referred to below in explaining a method for selecting a candidate list of SCS's and antennas using a predetermined set of criteria.

Figure 10 is a simplified block diagram of a monitoring system in accordance with the present invention.

- 20 Figure 11 is a flowchart of a monitoring method in accordance with the present invention.

- Figures 12A-12P schematically depict various aspects of a presently preferred implementation of the invention. Many of these depict signal formats and structures in
25 accordance with the GSM specification. In particular,

Figure 12A schematically depicts a call setup "arrow diagram" for a mobile station-originating call;

Figure 12B schematically depicts the structure of a Random Access Burst according to the GSM specification;

- 30 Figure 12C depicts the format of an RR Channel Request Message;

Figure 12D depicts the Request reference fields in the Channel Required Message;

Figure 12E depicts the Frame Number according to the GSM specification;

Figure 12F depicts Encryption Information Element within the Channel Activation Command;

Figure 12G depicts the Channel Number Information Element;

Figure 12H depicts the Channel Description Information Element;

5 Figure 12I depicts the Bit Pattern specified for CM Service Types;

Figure 12J depicts the MS Classmark Fields in a CM Service Request;

Figure 12K depicts the format of the Mobile Identity fields;

Figure 12L depicts Ciphering and Deciphering operations at the MS and BTS;

Figure 12M depicts a cascade of messages concerning Ciphering Transition among
10 the MSC, BSC, BTS and MS;

Figure 12N depicts an Encryption Information Element within the Encryption Command;

Figure 12O depicts a Called Party BCD Number; and

Figure 12P schematically depicts an exemplary system architecture for carrying out
15 the present invention.

20 DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

A goal of the present invention is to provide a mechanism for non-invasively collecting information concerning cell, frequency, and caller for purposes of directing a wireless location system. For example, the present invention provides a method that may be used in a Wireless Location System of the kind described below to locate GSM
25 mobile phones. With the architecture described below, the system would not be required to detect and demodulate messages from the mobile terminal during call setup. Instead, the WLS could ascertain call setup information from the interface between the BTS and the BSC, which is commonly called the "Abis" interface. From the Abis interface, the location system can identify the calling party (indirectly), the called party (e.g., 911), and
30 the TDMA/FDMA resource being used for a given call at any time.

The following is a description of an illustrative WLS of the kind in which the present invention may be used. This description is intended to provide the interested reader with a thorough understanding of a presently preferred environment in which the present invention may be utilized. It should be noted, however, that, except to the extent that

5 they may be expressly so limited, the claims of the present application are by no means limited to the details of the illustrative WLS described herein. Indeed, for example, the present invention is applicable to Wireless Location Systems characterized as TDOA systems, AOA systems, and hybrid TDOA/AOA systems. Following the description of the illustrative WLS, presently preferred embodiments of the inventive method for non-

10 invasively collecting call information are described.

Overview of WLS

A Wireless Location System, or WLS, may be configured to operate as a passive overlay to a wireless communications system, such as a cellular, PCS, or ESMR system,

15 although the concepts are not limited to just those types of communications systems. Wireless communications systems are generally not suitable for locating wireless devices because the designs of the wireless transmitters and cell sites do not include the necessary functionality to achieve accurate location. Accurate location in this application is defined as accuracy of 100 to 400 feet RMS (root mean square). This is distinguished

20 from the location accuracy that can be achieved by existing cell sites, which is generally limited to the radius of the cell site. In general, cell sites are not designed or programmed to cooperate between and among themselves to determine wireless transmitter location. Additionally, wireless transmitters such as cellular and PCS telephones are designed to be low cost and therefore generally do not have locating capability built-in. A WLS may

25 be designed to be a low cost addition to a wireless communications system that involves minimal changes to cell sites and no changes at all to standard wireless transmitters. The system may be considered passive because it does not contain transmitters, and therefore does not cause interference to the wireless communications system.

30 As shown in Figure 1, the Wireless Location System has four major kinds of subsystems: the Signal Collection Systems (SCS's) 10, the TDOA Location Processors (TLP's) 12, the Application Processors (AP's) 14, and the Network Operations Console (NOC) 16.

Each SCS is responsible for receiving the RF signals transmitted by the wireless transmitters on both control channels and voice channels. In general, each SCS is preferably installed at a wireless carrier's cell site, and therefore operates in parallel to a base station. Each TLP 12 is responsible for managing a network of SCS's 10 and for

5 providing a centralized pool of digital signal processing (DSP) resources that can be used in the location calculations. The SCS's 10 and the TLP's 12 operate together to determine the location of the wireless transmitters, as will be discussed more fully below. Digital signal processing is the preferable manner in which to process radio signals because DSP's are relatively low cost, provide consistent performance, and are easily re-

10 programmable to handle many different tasks. Both the SCS's 10 and TLP's 12 contain a significant amount of DSP resources, and the software in these systems can operate dynamically to determine where to perform a particular processing function based upon tradeoffs in processing time, communications time, queuing time, and cost. Each TLP 12 exists centrally primarily to reduce the overall cost of implementing the Wireless

15 Location System, although the techniques discussed herein are not limited to the preferred architecture shown. That is, DSP resources can be relocated within the Wireless Location System without changing the basic concepts and functionality disclosed.

20 The AP's 14 are responsible for managing all of the resources in the Wireless Location System, including all of the SCS's 10 and TLP's 12. Each AP 14 also contains a specialized database that contains "triggers" for the Wireless Location System. In order to conserve resources, the Wireless Location System can be programmed to locate only certain pre-determined types of transmissions. When a transmission of a pre-determined

25 type occurs, then the Wireless Location System is triggered to begin location processing. Otherwise, the Wireless Location System may be programmed to ignore the transmission. Each AP 14 also contains applications interfaces that permit a variety of applications to securely access the Wireless Location System. These applications may, for example, access location records in real time or non-real time, create or delete certain

30 type of triggers, or cause the Wireless Location System to take other actions. Each AP 14 is also capable of certain post-processing functions that allow the AP 14 to combine a

number of location records to generate extended reports or analyses useful for applications such as traffic monitoring or RF optimization.

The NOC 16 is a network management system that provides operators of the Wireless Location System easy access to the programming parameters of the Wireless Location System. For example, in some cities, the Wireless Location System may contain many hundreds or even thousands of SCS's 10. The NOC is the most effective way to manage a large Wireless Location System, using graphical user interface capabilities. The NOC will also receive real time alerts if certain functions within the Wireless Location System are not operating properly. These real time alerts can be used by the operator to take corrective action quickly and prevent a degradation of location service. Experience with trials of the Wireless Location System show that the ability of the system to maintain good location accuracy over time is directly related to the operator's ability to keep the system operating within its predetermined parameters.

Readers of U.S. Patents 5,327,144 and 5,608,410 and this specification will note similarities between the respective systems. Indeed, the system disclosed herein is significantly based upon and also significantly enhanced from the system described in those previous patents. For example, the SCS 10 has been expanded and enhanced from the Antenna Site System described in U.S. Patent No. 5,608,410. The SCS 10 now has the capability to support many more antennas at a single cell site, and further can support the use of extended antennas as described below. This enables the SCS 10 to operate with the sectorized cell sites now commonly used. The SCS 10 can also transfer data from multiple antennas at a cell site to the TLP 12 instead of always combining data from multiple antennas before transfer. Additionally, the SCS 10 can support multiple air interface protocols thereby allowing the SCS 10 to function even as a wireless carrier continually changes the configuration of its system.

The TLP 12 is similar to the Central Site System disclosed in 5,608,410, but has also been expanded and enhanced. For example, the TLP 12 has been made scaleable so that the amount of DSP resources required by each TLP 12 can be appropriately scaled to match the number of locations per second required by customers of the Wireless

Location System. In order to support scaling for different Wireless Location System capacities, a networking scheme has been added to the TLP 12 so that multiple TLP's 12 can cooperate to share RF data across wireless communication system network boundaries. Additionally, the TLP 12 has been given control means to determine the SCS's 10, and more importantly the antennas at each of the SCS's 10, from which the TLP 12 is to receive data in order to process a specific location. Previously, the Antenna Site Systems automatically forwarded data to the Central Site System, whether requested or not by the Central Site System. Furthermore, the SCS 10 and TLP 12 combined have been designed with additional means for removing multipath from the received transmissions.

The Database Subsystem of the Central Site System has been expanded and developed into the AP 14. The AP 14 can support a greater variety of applications than previously disclosed in 5,608,410, including the ability to post-process large volumes of location records from multiple wireless transmitters. This post-processed data can yield, for example, very effective maps for use by wireless carriers to improve and optimize the RF design of the communications systems. This can be achieved, for example, by plotting the locations of all of the callers in an area and the received signal strengths at a number of cell sites. The carrier can then determine whether each cell site is, in fact, serving the exact coverage area desired by the carrier. The AP 14 can also now store location records anonymously, that is, with the MIN and/or other identity information removed from the location record, so that the location record can be used for RF optimization or traffic monitoring without causing concerns about an individual user's privacy.

As shown in Figure 1A, a presently preferred implementation of the Wireless Location System includes a plurality of SCS regions each of which comprises multiple SCS's 10. For example, "SCS Region 1" includes SCS's 10A and 10B (and preferably others, not shown) that are located at respective cell sites and share antennas with the base stations at those cell sites. Drop and insert units 11A and 11B are used to interface fractional T1/E1 lines to full T1/E1 lines, which in turn are coupled to a digital access and control system (DACS) 13A. The DACS 13A and another DACS 13B are used in the manner described more fully below for communications between the SCS's 10A, 10B, etc., and

multiple TLP's 12A, 12B, etc. As shown, the TLP's are typically collocated and interconnected via an Ethernet network (backbone) and a second, redundant Ethernet network. Also coupled to the Ethernet networks are multiple AP's 14A and 14B, multiple NOC's 16A and 16B, and a terminal server 15. Routers 19A and 19B are used to couple
5 one Wireless Location System to one or more other Wireless Location System(s).

Signal Collection System 10

Generally, cell sites will have one of the following antenna configurations: (i) an omnidirectional site with 1 or 2 receive antennas or (ii) a sectorized site with 1, 2, or 3
10 sectors, and with 1 or 2 receive antennas used in each sector. As the number of cell sites has increased in the U.S. and internationally, sectorized cell sites have become the predominant configuration. However, there are also a growing number of micro-cells and pico-cells, which can be omnidirectional. Therefore, the SCS 10 has been designed to be configurable for any of these typical cell sites and has been provided with mechanisms to
15 employ any number of antennas at a cell site.

The basic architectural elements of the SCS 10 remain the same as for the Antenna Site System described in 5,608,410, but several enhancements have been made to increase the flexibility of the SCS 10 and to reduce the commercial deployment cost of the system.
20 The most presently preferred embodiment of the SCS 10 is described herein. The SCS 10, an overview of which is shown in Figure 2, includes digital receiver modules 10-2A through 10-2C; DSP modules 10-3A through 10-3C; a serial bus 10-4, a control and communications module 10-5; a GPS module 10-6; and a clock distribution module 10-7. The SCS 10 has the following external connections: power, fractional T1/E1
25 communications, RF connections to antennas, and a GPS antenna connection for the timing generation (or clock distribution) module 10-7. The architecture and packaging of the SCS 10 permit it to be physically collocated with cell sites (which is the most common installation place), located at other types of towers (such as FM, AM, two-way emergency communications, television, etc.), or located at other building structures (such
30 as rooftops, silos, etc.).

Timing Generation

The Wireless Location System depends upon the accurate determination of time at all SCS's 10 contained within a network. Several different timing generation systems have been described in previous disclosures, however the most presently preferred
5 embodiment is based upon an enhanced GPS receiver 10-6. The enhanced GPS receiver differs from most traditional GPS receivers in that the receiver contains algorithms that remove some of the timing instability of the GPS signals, and guarantees that any two SCS's 10 contained within a network can receive timing pulses that are within approximately ten nanoseconds of each other. These enhanced GPS receivers are now
10 commercially available, and further reduce some of the time reference related errors that were observed in previous implementations of wireless location systems. While this enhanced GPS receiver can produce a very accurate time reference, the output of the receiver may still have an unacceptable phase noise. Therefore, the output of the receiver is input to a low phase noise, crystal oscillator-driven phase locked loop circuit that can
15 now produce 10 MHz and one pulse per second (PPS) reference signals with less than 0.01 degrees RMS of phase noise, and with the pulse output at any SCS 10 in a Wireless Location System network within ten nanoseconds of any other pulse at another SCS 10. This combination of enhanced GPS receiver, crystal oscillator, and phase locked loop is now the most preferred method to produce stable time and frequency reference signals
20 with low phase noise.

The SCS 10 has been designed to support multiple frequency bands and multiple carriers with equipment located at the same cell site. This can take place by using multiple receivers internal to a single SCS chassis, or by using multiple chassis each with separate
25 receivers. In the event that multiple SCS chassis are placed at the same cell site, the SCS's 10 can share a single timing generation/clock distribution circuit 10-7 and thereby reduce overall system cost. The 10 MHz and one PPS output signals from the timing generation circuit are amplified and buffered internal to the SCS 10, and then made available via external connectors. Therefore a second SCS can receive its timing from a
30 first SCS using the buffered output and the external connectors. These signals can also be made available to base station equipment collocated at the cell site. This might be useful

to the base station, for example, in improving the frequency re-use pattern of a wireless communications system.

Receiver Module 10-2 (Wideband Embodiment)

5 When a wireless transmitter makes a transmission, the Wireless Location System must receive the transmission at multiple SCS's 10 located at multiple geographically dispersed cell sites. Therefore, each SCS 10 has the ability to receive a transmission on any RF channel on which the transmission may originate. Additionally, since the SCS 10 is capable of supporting multiple air interface protocols, the SCS 10 also supports
10 multiple types of RF channels. This is in contrast to most current base station receivers, which typically receive only one type of channel and are usually capable of receiving only on select RF channels at each cell site. For example, a typical TDMA base station receiver will only support 30 KHz wide channels, and each receiver is programmed to receive signals on only a single channel whose frequency does not change often (i.e.
15 there is a relatively fixed frequency plan). Therefore, very few TDMA base station receivers would receive a transmission on any given frequency. As another example, even though some GSM base station receivers are capable of frequency hopping, the receivers at multiple base stations are generally not capable of simultaneously tuning to a single frequency for the purpose of performing location processing. In fact, the receivers
20 at GSM base stations are programmed to frequency hop to avoid using an RF channel that is being used by another transmitter so as to minimize interference.

The SCS receiver module 10-2 is preferably a dual wideband digital receiver that can receive the entire frequency band and all of the RF channels of an air interface. For
25 cellular systems in the U.S., this receiver module is either 15 MHz wide or 25 MHz wide so that all of the channels of a single carrier or all of the channels of both carriers can be received. This receiver module has many of the characteristics of the receiver previously described in Patent Number 5,608,410, and Figure 2A is a block diagram of the currently preferred embodiment. Each receiver module contains an RF tuner section 10-2-1, a data
30 interface and control section 10-2-2 and an analog to digital conversion section 10-2-3. The RF tuner section 10-2-1 includes two full independent digital receivers (including Tuner #1 and Tuner #2) that convert the analog RF input from an external connector into

a digitized data stream. Unlike most base station receivers, the SCS receiver module does not perform diversity combining or switching. Rather, the digitized signal from each independent receiver is made available to the location processing. The present inventors have determined that there is an advantage to the location processing, and especially the multipath mitigation processing, to independently process the signals from each antenna rather than perform combining on the receiver module.

The receiver module 10-2 performs, or is coupled to elements that perform, the following functions: automatic gain control (to support both nearby strong signals and far away weak signals), bandpass filtering to remove potentially interfering signals from outside of the RF band of interest, synthesis of frequencies needed for mixing with the RF signals to create an IF signal that can be sampled, mixing, and analog to digital conversion (ADC) for sampling the RF signals and outputting a digitized data stream having an appropriate bandwidth and bit resolution. The frequency synthesizer locks the synthesized frequencies to the 10 MHz reference signal from the clock distribution/timing generation module 10-7 (Figure 2). All of the circuits used in the receiver module maintain the low phase noise characteristics of the timing reference signal. The receiver module preferably has a spurious free dynamic range of at least 80 dB.

The receiver module 10-2 also contains circuits to generate test frequencies and calibration signals, as well as test ports where measurements can be made by technicians during installation or troubleshooting. Various calibration processes are described in further detail below. The internally generated test frequencies and test ports provide an easy method for engineers and technicians to rapidly test the receiver module and diagnose any suspected problems. This is also especially useful during the manufacturing process.

One of the advantages of the Wireless Location System described herein is that no new antennas are required at cell sites. The Wireless Location System can use the existing antennas already installed at most cell sites, including both omni-directional and sectorized antennas. This feature can result in significant savings in the installation and

5 maintenance costs of the Wireless Location System versus other approaches that have been described in the prior art. The SCS's digital receivers 10-2 can be connected to the existing antennas in two ways, as shown in Figures 2B and 2C, respectively. In Figure 2B, the SCS receivers 10-2 are connected to the existing cell site multi-coupler or RF splitter. In this manner, the SCS 10 uses the cell site's existing low noise pre-amplifier, band pass filter, and multi-coupler or RF splitter. This type of connection usually limits the SCS 10 to supporting the frequency band of a single carrier. For example, an A-side cellular carrier will typically use the band pass filter to block signals from customers of the B-side carrier, and vice versa.

10

In Figure 2C, the existing RF path at the cell site has been interrupted, and a new pre-amplifier, band pass filter, and RF splitter has been added as part of the Wireless Location System. The new band pass filter will pass multiple contiguous frequency bands, such as both the A-side and B-side cellular carriers, thereby allowing the Wireless Location System to locate wireless transmitters using both cellular systems but using the antennas from a single cell site. In this configuration, the Wireless Location System uses matched RF components at each cell site, so that the phase versus frequency responses are identical. This is in contrast to existing RF components, which may be from different manufacturers or using different model numbers at various cell sites. Matching the response characteristics of RF components reduces a possible source of error for the location processing, although the Wireless Location System has the capability to compensate for these sources of error. Finally, the new pre-amplifier installed with the Wireless Location System will have a very low noise figure to improve the sensitivity of the SCS 10 at a cell site. The overall noise figure of the SCS digital receivers 10-2 is dominated by the noise figure of the low noise amplifiers. Because the Wireless Location System can use weak signals in location processing, whereas the base station typically cannot process weak signals, the Wireless Location System can significantly benefit from a high quality, very low noise amplifier.

30 In order to improve the ability of the Wireless Location System to accurately determine TDOA for a wireless transmission, the phase versus frequency response of the cell site's RF components are determined at the time of installation and updated at other certain

times and then stored in a table in the Wireless Location System. This can be important because, for example, the band pass filters and/or multi-couplers made by some manufacturers have a steep and non-linear phase versus frequency response near the edge of the pass band. If the edge of the pass band is very near to or coincident with the reverse control or voice channels, then the Wireless Location System would make incorrect measurements of the transmitted signal's phase characteristics if the Wireless Location System did not correct the measurements using the stored characteristics. This becomes even more important if a carrier has installed multi-couplers and/or band pass filters from more than one manufacturer, because the characteristics at each site may be different. In addition to measuring the phase versus frequency response, other environmental factors may cause changes to the RF path prior to the ADC. These factors require occasional and sometimes periodic calibration in the SCS 10.

Alternative Narrowband Embodiment of Receiver Module 10-2

In addition or as an alternative to the wideband receiver module, the SCS 10 also supports a narrowband embodiment of the receiver module 10-2. In contrast to the wideband receiver module that can simultaneously receive all of the RF channels in use by a wireless communications system, the narrowband receiver can only receive one or a few RF channels at a time. For example, the SCS 10 supports a 60 KHz narrowband receiver for use in AMPS/TDMA systems, covering two contiguous 30 KHz channels. This receiver is still a digital receiver as described for the wideband module, however the frequency synthesizing and mixing circuits are used to dynamically tune the receiver module to various RF channels on command. This dynamic tuning can typically occur in one millisecond or less, and the receiver can dwell on a specific RF channel for as long as required to receive and digitize RF data for location processing.

The purpose of the narrowband receiver is to reduce the implementation cost of a Wireless Location System from the cost that is incurred with wideband receivers. Of course, there is some loss of performance, but the availability of these multiple receivers permits wireless carriers to have more cost/performance options. Additional inventive functions and enhancements have been added to the Wireless Location System to support this new type of narrowband receiver. When the wideband receiver is being used, all RF

channels are received continuously at all SCS's 10, and subsequent to the transmission, the Wireless Location System can use the DSP's 10-3 (Figure 2) to dynamically select any RF channel from the digital memory. With the narrowband receiver, the Wireless Location System must ensure *a priori* that the narrowband receivers at multiple cell sites
5 are simultaneously tuned to the same RF channel so that all receivers can simultaneously receive, digitize and store the same wireless transmission. For this reason, the narrowband receiver is generally used only for locating voice channel transmissions, which can be known *a priori* to be making a transmission. Since control channel transmissions can occur asynchronously at any time, the narrowband receiver may not be
10 tuned to the correct channel to receive the transmission.

When the narrowband receivers are used for locating AMPS voice channel transmissions, the Wireless Location System has the ability to temporarily change the modulation characteristics of the AMPS wireless transmitter to aid location processing.
15 This may be necessary because AMPS voice channels are only FM modulated with the addition of a low level supervisory tone known as SAT. As is known in the art, the Cramer-Rao lower bound of AMPS FM modulation is significantly worse than the Manchester encoded FSK modulation used for AMPS reverse channels and "blank and burst" transmissions on the voice channel. Further, AMPS wireless transmitters may be
20 transmitting with significantly reduced energy if there is no modulating input signal (i.e., no one is speaking). To improve the location estimate by improving the modulation characteristics without depending on the existence or amplitude of an input modulating signal, the Wireless Location System can cause an AMPS wireless transmitter to transmit a "blank and burst" message at a point in time when the narrowband receivers at multiple
25 SCS's 10 are tuned to the RF channel on which the message will be sent. This is further described later.

The Wireless Location System performs the following steps when using the narrowband receiver module (see the flowchart of Figure 2C-1):

- 30 a first wireless transmitter is *a priori* engaged in transmitting on a particular RF channel;

the Wireless Location System triggers to make a location estimate of the first wireless transmitter (the trigger may occur either internally or externally via a command/response interface);

the Wireless Location System determines the cell site, sector, RF channel, timeslot,
5 long code mask, and encryption key (all information elements may not be necessary for all air interface protocols) currently in use by the first wireless transmitter;

the Wireless Location System tunes an appropriate first narrowband receiver at an appropriate first SCS 10 to the RF channel and timeslot at the designated cell site and sector, wherein appropriate typically means both available and collocated or
10 in closest proximity;

the first SCS 10 receives a time segment of RF data, typically ranging from a few microseconds to tens of milliseconds, from the first narrowband receiver and evaluates the transmission's power, SNR, and modulation characteristics;

15 if the transmission's power or SNR is below a predetermined threshold, the Wireless Location System waits a predetermined length of time and then returns to the above third step (where the Wireless Location System determines the cell site, sector, etc.);

if the transmission is an AMPS voice channel transmission and the modulation is
20 below a threshold, then the Wireless Location System commands the wireless communications system to send a command to the first wireless transmitter to cause a "blank and burst" on the first wireless transmitter;

the Wireless Location System requests the wireless communications system to prevent hand-off of the wireless transmitter to another RF channel for a
25 predetermined length of time;

the Wireless Location System receives a response from the wireless communications system indicating the time period during which the first wireless transmitter will be prevented from handing-off, and if commanded, the time period during which the wireless communications system will send a command to the first wireless
30 transmitter to cause a "blank and burst";

the Wireless Location System determines the list of antennas that will be used in location processing (the antenna selection process is described below);

the Wireless Location System determines the earliest Wireless Location System timestamp at which the narrowband receivers connected to the selected antennas are available to begin simultaneously collecting RF data from the RF channel currently in use by the first wireless transmitter;

5 based upon the earliest Wireless Location System timestamp and the time periods in the response from the wireless communications system, the Wireless Location System commands the narrowband receivers connected to the antennas that will be used in location processing to tune to the cell site, sector, and RF channel currently in use by the first wireless transmitter and to receive RF data for a

10 predetermined dwell time (based upon the bandwidth of the signal, SNR, and integration requirements);

the RF data received by the narrowband receivers are written into the dual port memory;

location processing on the received RF data commences, as described in Patent Nos.

15 5,327,144 and 5,608,410 and in sections below;

the Wireless Location System again determines the cell site, sector, RF channel, timeslot, long code mask, and encryption key currently in use by the first wireless transmitter;

if the cell site, sector, RF channel, timeslot, long code mask, and encryption key

20 currently in use by the first wireless transmitter has changed between queries (i.e. before and after gathering the RF data) the Wireless Location System ceases location processing, causes an alert message that location processing failed because the wireless transmitter changed transmission status during the period of time in which RF data was being received, and re-triggers this entire process;

25 location processing on the received RF data completes in accordance with the steps described below.

The determination of the information elements including cell site, sector, RF channel, timeslot, long code mask, and encryption key (all information elements may not be

30 necessary for all air interface protocols) is typically obtained by the Wireless Location System through a command / response interface between the Wireless Location System and the wireless communications system.

The use of the narrowband receiver in the manner described above is known as random tuning because the receivers can be directed to any RF channel on command from the system. One advantage to random tuning is that locations are processed only for those
5 wireless transmitters for which the Wireless Location System is triggered. One disadvantage to random tuning is that various synchronization factors, including the interface between the wireless communications system and the Wireless Location System and the latency times in scheduling the necessary receivers throughout the system, can limit the total location processing throughput. For example, in a TDMA
10 system, random tuning used throughout the Wireless Location System will typically limit location processing throughput to about 2.5 locations per second per cell site sector.

Therefore, the narrowband receiver also supports another mode, known as automatic sequential tuning, which can perform location processing at a higher throughput. For
15 example, in a TDMA system, using similar assumptions about dwell time and setup time as for the narrowband receiver operation described above, sequential tuning can achieve a location processing throughput of about 41 locations per second per cell site sector, meaning that all 395 TDMA RF channels can be processed in about 9 seconds. This increased rate can be achieved by taking advantage of, for example, the two contiguous
20 RF channels that can be received simultaneously, location processing all three TDMA timeslots in an RF channel, and eliminating the need for synchronization with the wireless communications system. When the Wireless Location System is using the narrowband receivers for sequential tuning, the Wireless Location System has no knowledge of the identity of the wireless transmitter because the Wireless Location
25 System does not wait for a trigger, nor does the Wireless Location System query the wireless communications system for the identity information prior to receiving the transmission. In this method, the Wireless Location System sequences through every cell site, RF channel and time slot, performs location processing, and reports a location record identifying a time stamp, cell site, RF channel, time slot, and location. Subsequent
30 to the location record report, the Wireless Location System and the wireless communications system match the location records to the wireless communications system's data indicating which wireless transmitters were in use at the time, and which

cell sites, RF channels, and time slots were used by each wireless transmitter. Then, the Wireless Location System can retain the location records for wireless transmitters of interest, and discard those location records for the remaining wireless transmitters.

5 Digital Signal Processor Module 10-3

The SCS digital receiver modules 10-2 output a digitized RF data stream having a specified bandwidth and bit resolution. For example, a 15 MHz embodiment of the wideband receiver may output a data stream containing 60 million samples per second, at a resolution of 14 bits per sample. This RF data stream will contain all of the RF

10 channels that are used by the wireless communications system. The DSP modules 10-3 receive the digitized data stream, and can extract any individual RF channel through digital mixing and filtering. The DSP's can also reduce the bit resolution upon command from the Wireless Location System, as needed to reduce the bandwidth requirements between the SCS 10 and TLP 12. The Wireless Location System can dynamically select

15 the bit resolution at which to forward digitized baseband RF data, based upon the processing requirements for each location. DSP's are used for these functions to reduce the systemic errors that can occur from mixing and filtering with analog components. The use of DSP's allows perfect matching in the processing between any two SCS's 10.

20 A block diagram of the DSP module 10-3 is shown in Figure 2D, and the operation of the DSP module is depicted by the flowchart of Figure 2E. As shown in Figure 2D, the DSP module 10-3 comprises the following elements: a pair of DSP elements 10-3-1A and 10-3-1B, referred to collectively as a "first" DSP; serial to parallel converters 10-3-2; dual port memory elements 10-3-3; a second DSP 10-3-4; a parallel to serial converter; a

25 FIFO buffer; a DSP 10-3-5 (including RAM) for detection, another DSP 10-3-6 for demodulation, and another DSP 10-3-7 for normalization and control; and an address generator 10-3-8. In a presently preferred embodiment, the DSP module 10-3 receives the wideband digitized data stream (Figure 2E, step S1), and uses the first DSP (10-3-1A and 10-3-1B) to extract blocks of channels (step S2). For example, a first DSP

30 programmed to operate as a digital drop receiver can extract four blocks of channels, wherein each block includes at least 1.25 MHz of bandwidth. This bandwidth can include 42 channels of AMPS or TDMA, 6 channels of GSM, or 1 channel of CDMA.

The DSP does not require the blocks to be contiguous, as the DSP can independently digitally tune to any set of RF channels within the bandwidth of the wideband digitized data stream. The DSP can also perform wideband or narrow band energy detection on all or any of the channels in the block, and report the power levels by channel to the TLP 12 (step S3). For example, every 10 ms, the DSP can perform wideband energy detection and create an RF spectral map for all channels for all receivers (see step S9). Because this spectral map can be sent from the SCS 10 to the TLP 12 every 10 ms via the communications link connecting the SCS 10 and the TLP 12, a significant data overhead could exist. Therefore, the DSP reduces the data overhead by companding the data into a finite number of levels. Normally, for example, 84 dB of dynamic range could require 14 bits. In the companding process implemented by the DSP, the data is reduced, for example, to only 4 bits by selecting 16 important RF spectral levels to send to the TLP 12. The choice of the number of levels, and therefore the number of bits, as well as the representation of the levels, can be automatically adjusted by the Wireless Location System. These adjustments are performed to maximize the information value of the RF spectral messages sent to the TLP 12 as well as to optimize the use of the bandwidth available on the communications link between the SCS 10 and the TLP 12.

After conversion, each block of RF channels (each at least 1.25 MHz) is passed through serial to parallel converter 10-3-2 and then stored in dual port digital memory 10-3-3 (step S4). The digital memory is a circular memory, which means that the DSP module begins writing data into the first memory address and then continues sequentially until the last memory address is reached. When the last memory address is reached, the DSP returns to the first memory address and continues to sequentially write data into memory. Each DSP module typically contains enough memory to store several seconds of data for each block of RF channels to support the latency and queuing times in the location process.

In the DSP module, the memory address at which digitized and converted RF data is written into memory is the time stamp used throughout the Wireless Location System and which the location processing references in determining TDOA. In order to ensure that the time stamps are aligned at every SCS 10 in the Wireless Location System, the

address generator 10-3-8 receives the one pulse per second signal from the timing generation/clock distribution module 10-7 (Figure 2). Periodically, the address generator at all SCS's 10 in a Wireless Location System will simultaneously reset themselves to a known address. This enables the location processing to reduce or eliminate accumulated timing errors in the recording of time stamps for each digitized data element.

The address generator 10-3-8 controls both writing to and reading from the dual port digital memory 10-3-3. Writing takes places continuously since the ADC is continuously sampling and digitizing RF signals and the first DSP (10-3-1A and 10-3-1B) is continuously performing the digital drop receiver function. However, reading occurs in bursts as the Wireless Location System requests data for performing demodulation and location processing. The Wireless Location System may even perform location processing recursively on a single transmission, and therefore requires access to the same data multiple times. In order to service the many requirements of the Wireless Location System, the address generator allows the dual port digital memory to be read at a rate faster than the writing occurs. Typically, reading can be performed eight times faster than writing.

The DSP module 10-3 uses the second DSP 10-3-4 to read the data from the digital memory 10-3-3, and then performs a second digital drop receiver function to extract baseband data from the blocks of RF channels (step S5). For example, the second DSP can extract any single 30 KHz AMPS or TDMA channel from any block of RF channels that have been digitized and stored in the memory. Likewise, the second DSP can extract any single GSM channel. The second DSP is not required to extract a CDMA channel, since the channel bandwidth occupies the full bandwidth of the stored RF data. The combination of the first DSP 10-3-1A, 10-3-1B and the second DSP 10-3-4 allows the DSP module to select, store, and recover any single RF channel in a wireless communications system. A DSP module typically will store four blocks of channels. In a dual-mode AMPS/TDMA system, a single DSP module can continuously and simultaneously monitor up to 42 analog reverse control channels, up to 84 digital control channels, and also be tasked to monitor and locate any voice channel transmission. A single SCS chassis will typically support up to three receiver modules 10-2 (Figure 2), to

cover three sectors of two antennas each, and up to nine DSP modules (three DSP modules per receiver permits an entire 15 MHz bandwidth to be simultaneously stored into digital memory). Thus, the SCS 10 is a very modular system than can be easily scaled to match any type of cell site configuration and processing load.

5

The DSP module 10-3 also performs other functions, including automatic detection of active channels used in each sector (step S6), demodulation (step S7), and station based location processing (step S8). The Wireless Location System maintains an active map of the usage of the RF channels in a wireless communications system (step S9), which
10 enables the Wireless Location System to manage receiver and processing resources, and to rapidly initiate processing when a particular transmission of interest has occurred. The active map comprises a table maintained within the Wireless Location System that lists for each antenna connected to an SCS 10 the primary channels assigned to that SCS 10 and the protocols used in those channels. A primary channel is an RF control channel
15 assigned to a collocated or nearby base station which the base station uses for communications with wireless transmitters. For example, in a typical cellular system with sectorized cell sites, there will be one RF control channel frequency assigned for use in each sector. Those control channel frequencies would typically be assigned as primary channels for a collocated SCS 10.

20

The same SCS 10 may also be assigned to monitor the RF control channels of other nearby base stations as primary channels, even if other SCS's 10 also have the same primary channels assigned. In this manner, the Wireless Location System implements a system demodulation redundancy that ensures that any given wireless transmission has
25 an infinitesimal probability of being missed. When this demodulation redundancy feature is used, the Wireless Location System will receive, detect, and demodulate the same wireless transmission two or more times at more than one SCS 10. The Wireless Location System includes means to detect when this multiple demodulation has occurred and to trigger location processing only once. This function conserves the processing and
30 communications resources of the Wireless Location System, and is further described below. This ability for a single SCS 10 to detect and demodulate wireless transmissions occurring at cell sites not collocated with the SCS 10 permits operators of the Wireless

Location System to deploy more efficient Wireless Location System networks. For example, the Wireless Location System may be designed such that the Wireless Location System uses much fewer SCS's 10 than the wireless communications system has base stations.

5

In the Wireless Location System, primary channels are entered and maintained in the table using two methods: direct programming and automatic detection. Direct programming comprises entering primary channel data into the table using one of the Wireless Location System user interfaces, such as the Network Operations Console 16 (Figure 1), or by receiving channel assignment data from the Wireless Location System to wireless communications system interface. Alternatively, the DSP module 10-3 also runs a background process known as automatic detection in which the DSP uses spare or scheduled processing capacity to detect transmissions on various possible RF channels and then attempt to demodulate those transmissions using probable protocols. The DSP module can then confirm that the primary channels directly programmed are correct, and can also quickly detect changes made to channels at base station and send an alert to the operator of the Wireless Location System.

The DSP module performs the following steps in automatic detection (see Figure 2E-1):

- 20 for each possible control and/or voice channel which may be used in the coverage area of the SCS 10, peg counters are established (step S7-1);
- at the start of a detection period, all peg counters are reset to zero (step S7-2);
- each time that a transmission occurs in a specified RF channel, and the received power level is above a particular pre-set threshold, the peg counter for that channel
- 25 is incremented (step S7-3);
- each time that a transmission occurs in a specified RF channel, and the received power level is above a second particular pre-set threshold, the DSP module attempts to demodulate a certain portion of the transmission using a first preferred protocol (step S7-4);
- 30 if the demodulation is successful, a second peg counter for that channel is incremented (step S7-5);

- if the demodulation is unsuccessful, the DSP module attempts to demodulate a portion of the transmission using a second preferred protocol (step S7-6);
if the demodulation is successful, a third peg counter for that channel is incremented (step S7-7);
- 5 at the end of a detection period, the Wireless Location System reads all peg counters (step S7-8); and
the Wireless Location System automatically assigns primary channels based upon the peg counters (step S7-9).
- 10 The operator of the Wireless Location System can review the peg counters and the automatic assignment of primary channels and demodulation protocols, and override any settings that were performed automatically. In addition, if more than two preferred protocols may be used by the wireless carrier, then the DSP module 10-3 can be downloaded with software to detect the additional protocols. The architecture of the SCS
- 15 10, based upon wideband receivers 10-2, DSP modules 10-3, and downloadable software permits the Wireless Location System to support multiple demodulation protocols in a single system. There is a significant cost advantage to supporting multiple protocols within the single system, as only a single SCS 10 is required at a cell site. This is in contrast to many base station architectures, which may require different transceiver
- 20 modules for different modulation protocols. For example, while the SCS 10 could support AMPS, TDMA, and CDMA simultaneously in the same SCS 10, there is no base station currently available that can support this functionality.

The ability to detect and demodulate multiple protocols also includes the ability to

25 independently detect the use of authentication in messages transmitted over the certain air interface protocols. The use of authentication fields in wireless transmitters started to become prevalent within the last few years as a means to reduce the occurrence of fraud in wireless communications systems. However, not all wireless transmitters have implemented authentication. When authentication is used, the protocol generally inserts

30 an additional field into the transmitted message. Frequently this field is inserted between the identity of the wireless transmitter and the dialed digits in the transmitted message. When demodulating a wireless transmission, the Wireless Location System determines

the number of fields in the transmitted message, as well as the message type (i.e. registration, origination, page response, etc.). The Wireless Location System demodulates all fields and if extra fields appear to be present, giving consideration to the type of message transmitted, then the Wireless Location System tests all fields for a trigger condition. For example, if the dialed digits "911" appear in the proper place in a field, and the field is located either in its proper place without authentication or its proper place with authentication, then the Wireless Location System triggers normally. In this example, the digits "911" would be required to appear in sequence as "911" or "*911", with no other digits before or after either sequence. This functionality reduces or eliminates a false trigger caused by the digits "911" appearing as part of an authentication field.

The support for multiple demodulation protocols is important for the Wireless Location System to successfully operate because location processing must be quickly triggered when a wireless caller has dialed "911". The Wireless Location System can trigger location processing using two methods: the Wireless Location System will independently demodulate control channel transmissions, and trigger location processing using any number of criteria such as dialed digits, or the Wireless Location System may receive triggers from an external source such as the carrier's wireless communications system. The present inventors have found that independent demodulation by the SCS 10 results in the fastest time to trigger, as measured from the moment that a wireless user presses the "SEND" or "TALK" (or similar) button on a wireless transmitter.

Control and Communications Module 10-5

The control and communications module 10-5, depicted in Figure 2F, includes data buffers 10-5-1, a controller 10-5-2, memory 10-5-3, a CPU 10-5-4 and a T1/E1 communications chip 10-5-5. The module has many of the characteristics previously described in Patent Number 5,608,410. Several enhancements have been added in the present embodiment. For example, the SCS 10 now includes an automatic remote reset capability, even if the CPU on the control and communications module ceases to execute its programmed software. This capability can reduce the operating costs of the Wireless Location System because technicians are not required to travel to a cell site to reset an

- SCS 10 if it fails to operate normally. The automatic remote reset circuit operates by monitoring the communications interface between the SCS 10 and the TLP 12 for a particular sequence of bits. This sequence of bits is a sequence that does not occur during normal communications between the SCS 10 and the TLP 12. This sequence, for
- 5 example, may consist of an all ones pattern. The reset circuit operates independently of the CPU so that even if the CPU has placed itself in a locked or other non-operating status, the circuit can still achieve the reset of the SCS 10 and return the CPU to an operating status.
- 10 This module now also has the ability to record and report a wide variety of statistics and variables used in monitoring or diagnosing the performance of the SCS 10. For example, the SCS 10 can monitor the percent capacity usage of any DSP or other processor in the SCS 10, as well as the communications interface between the SCS 10 and the TLP 12. These values are reported regularly to the AP 14 and the NOC 16, and are used to
- 15 determine when additional processing and communications resources are required in the system. For example, alarm thresholds may be set in the NOC to indicate to an operator if any resource is consistently exceeding a preset threshold. The SCS 10 can also monitor the number of times that transmissions have been successfully demodulated, as well as the number of failures. This is useful in allowing operators to determine whether the
- 20 signal thresholds for demodulation have been set optimally.

This module, as well as the other modules, can also self-report its identity to the TLP 12. As described below, many SCS's 10 can be connected to a single TLP 12. Typically, the communications between SCS's 10 and TLP's 12 is shared with the communications

25 between base stations and MSC's. It is frequently difficult to quickly determine exactly which SCS's 10 have been assigned to particular circuits. Therefore, the SCS 10 contains a hard coded identity, which is recorded at the time of installation. This identity can be read and verified by the TLP 12 to positively determine which SCS 10 has been assigned by a carrier to each of several different communications circuits.

30

The SCS to TLP communications supports a variety of messages, including: commands and responses, software download, status and heartbeat, parameter download, diagnostic,

spectral data, phase data, primary channel demodulation, and RF data. The communications protocol is designed to optimize Wireless Location System operation by minimizing the protocol overhead and the protocol includes a message priority scheme. Each message type is assigned a priority, and the SCS 10 and the TLP 12 will queue

5 messages by priority such that a higher priority message is sent before a lower priority message is sent. For example, demodulation messages are generally set at a high priority because the Wireless Location System must trigger location processing on certain types of calls (i.e., E9-1-1) without delay. Although higher priority messages are queued before lower priority messages, the protocol generally does not preempt a message that is

10 already in transit. That is, a message in the process of being sent across the SCS 10 to TLP 12 communications interface will be completed fully, but then the next message to be sent will be the highest priority message with the earliest time stamp. In order to minimize the latency of high priority messages, long messages, such as RF data, are sent in segments. For example, the RF data for a full 100-millisecond AMPS transmission

15 may be separated into 10-millisecond segments. In this manner, a high priority message may be queued in between segments of the RF data.

Calibration and Performance Monitoring

The architecture of the SCS 10 is heavily based upon digital technologies

20 including the digital receiver and the digital signal processors. Once RF signals have been digitized, timing, frequency, and phase differences can be carefully controlled in the various processes. More importantly, any timing, frequency, and phase differences can be perfectly matched between the various receivers and various SCS's 10 used in the Wireless Location System. However, prior to the ADC, the RF signals pass through a

25 number of RF components, including antennas, cables, low noise amplifiers, filters, duplexors, multi-couplers, and RF splitters. Each of these RF components has characteristics important to the Wireless Location System, including delay and phase versus frequency response. When the RF and analog components are perfectly matched between the pairs of SCS's 10, such as SCS 10A and SCS 10B in Figure 2G, then the

30 effects of these characteristics are automatically eliminated in the location processing. But when the characteristics of the components are not matched, then the location processing can inadvertently include instrumental errors resulting from the mismatch.

Additionally, many of these RF components can experience instability with power, time, temperature, or other factors that can add instrumental errors to the determination of location. Therefore, several inventive techniques have been developed to calibrate the RF components in the Wireless Location System and to monitor the performance of the

5 Wireless Location System on a regular basis. Subsequent to calibration, the Wireless Location System stores the values of these delays and phases versus frequency response (i.e. by RF channel number) in a table in the Wireless Location System for use in correcting these instrumental errors. Figures 2G-2J are referred to below in explaining these calibration methods.

10

External Calibration Method

Referring to Figure 2G, the timing stability of the Wireless Location System is measured along baselines, wherein each baseline is comprised of two SCS's, 10A and 10B, and an imaginary line (A - B) drawn between them. In a TDOA / FDOA type of

15 Wireless Location System, locations of wireless transmitters are calculated by measuring the differences in the times that each SCS 10 records for the arrival of the signal from a wireless transmitter. Thus, it is important that the differences in times measured by SCS's 10 along any baseline are largely attributed to the transmission time of the signal from the wireless transmitter and minimally attributed to the variations in the RF and

20 analog components of the SCS's 10 themselves. To meet the accuracy goals of the Wireless Location System, the timing stability for any pair of SCS's 10 are maintained at much less than 100 nanoseconds RMS (root mean square). Thus, the components of the Wireless Location System will contribute less than 100 feet RMS of instrumentation error in the estimation of the location of a wireless transmitter. Some of this error is

25 allocated to the ambiguity of the signal used to calibrate the system. This ambiguity can be determined from the well-known Cramer-Rao lower bound equation. In the case of an AMPS reverse control channel, this error is approximately 40 nanoseconds RMS. The remainder of the error budget is allocated to the components of the Wireless Location System, primarily the RF and analog components in the SCS 10.

30

In the external calibration method, the Wireless Location System uses a network of calibration transmitters whose signal characteristics match those of the target wireless

- transmitters. These calibration transmitters may be ordinary wireless telephones emitting periodic registration signals and/or page response signals. Each usable SCS-to-SCS baseline is preferably calibrated periodically using a calibration transmitter that has a relatively clear and unobstructed path to both SCS's 10 associated with the baseline. The
- 5 calibration signal is processed identically to a signal from a target wireless transmitter. Since the TDOA values are known *a priori*, any errors in the calculations are due to systemic errors in the Wireless Location System. These systemic errors can then be removed in the subsequent location calculations for target transmitters.
- 10 Figure 2G illustrates the external calibration method for minimizing timing errors. As shown, a first SCS 10A at a point "A" and a second SCS 10A at a point "B" have an associated baseline A-B. A calibration signal emitted at time T_0 by a calibration transmitter at point "C" will theoretically reach first SCS 10A at time $T_0 + T_{AC}$. T_{AC} is a measure of the amount of time required for the calibration signal to travel from the
- 15 antenna on the calibration transmitter to the dual port digital memory in a digital receiver. Likewise, the same calibration signal will reach second SCS 10B at a theoretical time $T_0 + T_{BC}$. Usually, however, the calibration signal will not reach the digital memory and the digital signal processing components of the respective SCS's 10 at exactly the correct times. Rather, there will be errors e_1 and e_2 in the amount of time
- 20 (T_{AC} , T_{BC}) it takes the calibration signal to propagate from the calibration transmitter to the SCS's 10, respectively, such that the exact times of arrival are actually $T_0 + T_{AC} + e_1$ and $T_0 + T_{BC} + e_2$. Such errors will be due to some extent to delays in the signal propagation through the air, i.e., from the calibration transmitter's antenna to the SCS antennas; however, the errors will be due primarily to time varying characteristics in the
- 25 SCS front end components. The errors e_1 and e_2 cannot be determined *per se* because the system does not know the exact time (T_0) at which the calibration signal was transmitted. The system can, however, determine the error in the *difference* in the time of arrival of the calibration signal at the respective SCS's 10 of any given pair of SCS's 10. This TDOA error value is defined as the difference between the measured TDOA value
- 30 and the theoretical TDOA value τ_0 , wherein τ_0 is the theoretical differences between the theoretical delay values T_{AC} and T_{BC} . Theoretical TDOA values for each pair of SCS's

10 and each calibration transmitter are known because the positions of the SCS's 10 and calibration transmitter, and the speed at which the calibration signal propagates, are known. The measured TDOA baseline ($TDOA_{A-B}$) can be represented as $TDOA_{A-B} = \tau_0 + \epsilon$, wherein $\epsilon = e_1 - e_2$. In a similar manner, a calibration signal from a second
 5 calibration transmitter at point "D" will have associated errors e_3 and e_4 . The ultimate value of ϵ to be subtracted from TDOA measurements for a target transmitter will be a function (e.g., weighted average) of the ϵ values derived for one or more calibration transmitters. Therefore, a given TDOA measurement ($TDOA_{measured}$) for a pair of SCS's 10 at points "X" and "Y" and a target wireless transmitter at an unknown location will be
 10 corrected as follows:

$$\begin{aligned} TDOA_{X-Y} &= TDOA_{measured} - \epsilon \\ \epsilon &= k_1\epsilon_1 + k_2\epsilon_2 + \dots k_N\epsilon_N, \end{aligned}$$

15 where k_1, k_2 , etc., are weighting factors and ϵ_1, ϵ_2 , etc., are the errors determined by subtracting the measured TDOA values from the theoretical values for each calibration transmitter. In this example, error value ϵ_1 may be the error value associated with the calibration transmitter at point "C" in the drawing. The weighting factors are determined by the operator of the Wireless Location System, and input into the configuration tables
 20 for each baseline. The operator will take into consideration the distance from each calibration transmitter to the SCS's 10 at points "X" and "Y", the empirically determined line of sight from each calibration transmitter to the SCS's 10 at points "X" and "Y", and the contribution that each SCS "X" and "Y" would have made to a location estimate of a wireless transmitter that might be located in the vicinity of each calibration transmitter.
 25 In general, calibration transmitters that are nearer to the SCS's 10 at points "X" and "Y" will be weighted higher than calibration transmitters that are farther away, and calibration transmitters with better line of sight to the SCS's 10 at points "X" and "Y" will be weighted higher than calibration transmitters with worse line of sight.
 30 Each error component e_1, e_2 , etc., and therefore the resulting error component ϵ , can vary widely, and wildly, over time because some of the error component is due to

- 5 multipath reflection from the calibration transmitter to each SCS 10. The multipath reflection is very much path dependent and therefore will vary from measurement to measurement and from path to path. It is not an object of this method to determine the multipath reflection for these calibration paths, but rather to determine the portion of the errors that are attributable to the components of the SCS's 10. Typically, therefore, error values e1 and e3 will have a common component since they relate to the same first SCS 10A. Likewise, error values e2 and e4 will also have a common component since they relate to the second SCS 10B. It is known that while the multipath components can vary wildly, the component errors vary slowly and typically vary sinusoidally. Therefore, in the external calibration method, the error values ϵ are filtered using a weighted, time-based filter that decreases the weight of the wildly varying multipath components while preserving the relatively slow changing error components attributed to the SCS's 10. One such exemplary filter used in the external calibration method is the Kalman filter.
- 15 The period between calibration transmissions is varied depending on the error drift rates determined for the SCS components. The period of the drift rate should be much longer than the period of the calibration interval. The Wireless Location System monitors the period of the drift rate to determine continuously the rate of change, and may periodically adjust the calibration interval, if needed. Typically, the calibration rate for a Wireless Location System such as one in accordance with the present invention is between 10 and 30 minutes. This corresponds well with the typical time period for the registration rate in a wireless communications system. If the Wireless Location System were to determine that the calibration interval must be adjusted to a rate faster than the registration rate of the wireless communications system, then the AP 14 (Figure 1) would automatically force the calibration transmitter to transmit by paging the transmitter at the prescribed interval. Each calibration transmitter is individually addressable and therefore the calibration interval associated with each calibration transmitter can be different.
- 25

Since the calibration transmitters used in the external calibration method are standard telephones, the Wireless Location System must have a mechanism to distinguish those telephones from the other wireless transmitters that are being located for various

30

application purposes. The Wireless Location System maintains a list of the identities of the calibration transmitters, typically in the TLP 12 and in the AP 14. In a cellular system, the identity of the calibration transmitter can be the Mobile Identity Number, or MIN. When the calibration transmitter makes a transmission, the transmission is received
5 by each SCS 10 and demodulated by the appropriate SCS 10. The Wireless Location System compares the identity of the transmission with a pre-stored tasking list of identities of all calibration transmitters. If the Wireless Location System determines that the transmission was a calibration transmission, then the Wireless Location System initiates external calibration processing.

10

Internal Calibration Method

In addition to the external calibration method, it is an object of the present invention to calibrate all channels of the wideband digital receiver used in the SCS 10 of a Wireless Location System. The external calibration method will typically calibrate only
15 a single channel of the multiple channels used by the wideband digital receiver. This is because the fixed calibration transmitters will typically scan to the highest-power control channel, which will typically be the same control channel each time. The transfer function of a wideband digital receiver, along with the other associated components, does not remain perfectly constant, however, and will vary with time and temperature.
20 Therefore, even though the external calibration method can successfully calibrate a single channel, there is no assurance that the remaining channels will also be calibrated.

The internal calibration method, represented in the flowchart of Figure 2H, is particularly suited for calibrating an individual first receiver system (i.e., SCS 10) that is
25 characterized by a time- and frequency-varying transfer function, wherein the transfer function defines how the amplitude and phase of a received signal will be altered by the receiver system and the receiver system is utilized in a location system to determine the location of a wireless transmitter by, in part, determining a difference in time of arrival of a signal transmitted by the wireless transmitter and received by the receiver system to
30 be calibrated and another receiver system, and wherein the accuracy of the location estimate is dependent, in part, upon the accuracy of TDOA measurements made by the system. An example of a AMPS RCC transfer function is depicted in Figure 2I, which

depicts how the phase of the transfer function varies across the 21 control channels spanning 630 KHz.

Referring to Figure 2H, the internal calibration method includes the steps of temporarily
5 and electronically disconnecting the antenna used by a receiver system from the receiver system (step S-20); injecting an internally generated wideband signal with known and stable signal characteristics into the first receiver system (step S-21); utilizing the generated wideband signal to obtain an estimate of the manner in which the transfer function varies across the bandwidth of the first receiver system (step S-22); and utilizing
10 the estimate to mitigate the effects of the variation of the first transfer function on the time and frequency measurements made by the first receiver system (step S-23). One example of a stable wideband signal used for internal calibration is a comb signal, which is comprised of multiple individual, equal-amplitude frequency elements at a known spacing, such as 5 KHz. An example of such a signal is shown in Figure 2I.

15 The antenna must be temporarily disconnected during the internal calibration process to prevent external signals from entering the wideband receiver and to guarantee that the receiver is only receiving the stable wideband signal. The antenna is electronically disconnected only for a few milliseconds to minimize the chance of missing too much of
20 a signal from a wireless transmitter. In addition, internal calibration is typically performed immediately after external calibration to minimize the possibility that the any component in the SCS 10 drifts during the interval between external and internal calibration. The antenna is disconnected from the wideband receiver using two electronically controlled RF relays (not shown). An RF relay cannot provide perfect
25 isolation between input and output even when in the "off" position, but it can provide up to 70 dB of isolation. Two relays may be used in series to increase the amount of isolation and to further assure that no signal is leaked from the antenna to the wideband receiver during calibration. Similarly, when the internal calibration function is not being used, the internal calibration signal is turned off, and the two RF relays are also turned
30 off to prevent leakage of the internal calibration signals into the wideband receiver when the receiver is collecting signals from wireless transmitters.

The external calibration method provides an absolute calibration of a single channel and the internal calibration method then calibrates each other channel relative to the channel that had been absolutely calibrated. The comb signal is particularly suited as a stable wideband signal because it can be easily generated using a stored replica of the signal and a digital to analog converter.

External Calibration Using Wideband Calibration Signal

The external calibration method described next may be used in connection with an SCS receiver system characterized by a time- and frequency-varying transfer function, which preferably includes the antennas, filters, amplifiers, duplexors, multi-couplers, splitters, and cabling associated with the SCS receiver system. The method includes the step of transmitting a stable, known wideband calibration signal from an external transmitter. The wideband calibration signal is then used to estimate the transfer function across a prescribed bandwidth of the SCS receiver system. The estimate of the transfer function is subsequently employed to mitigate the effects of variation of the transfer function on subsequent TDOA/FDOA measurements. The external transmission is preferably of short duration and low power to avoid interference with the wireless communications system hosting the Wireless Location System.

In the preferred method, the SCS receiver system is synchronized with the external transmitter. Such synchronization may be performed using GPS timing units. Moreover, the receiver system may be programmed to receive and process the entire wideband of the calibration signal only at the time that the calibration signal is being sent. The receiver system will not perform calibration processing at any time other than when in synchronization with the external calibration transmissions. In addition, a wireless communications link is used between the receiver system and the external calibration transmitter to exchange commands and responses. The external transmitter may use a directional antenna to direct the wideband signal only at the antennas of the SCS receiver system. Such as directional antenna may be a Yagi antenna (i.e. linear end-fire array). The calibration method preferably includes making the external transmission only when the directional antenna is aimed at the receiver system's antennas and the risk of multipath reflection is low.

Calibrating for Station Biases

Another aspect of the present invention concerns a calibration method to correct for station biases in a SCS receiver system. The “station bias” is defined as the finite
5 delay between when an RF signal from a wireless transmitter reaches the antenna and when that same signal reached the wideband receiver. The inventive method includes the step of measuring the length of the cable from the antennas to the filters and determining the corresponding delays associated with the cable length. In addition, the method includes injecting a known signal into the filter, duplexor, multi-coupler, or RF splitter
10 and measuring the delay and phase response versus frequency response from the input of each device to the wideband receiver. The delay and phase values are then combined and used to correct subsequent location measurements. When used with the GPS based timing generation described above, the method preferably includes correcting for the GPS cable lengths. Moreover, an externally generated reference signal is preferably used
15 to monitor changes in station bias that may arise due to aging and weather. Finally, the station bias by RF channel and for each receiver system in the Wireless Location System is preferably stored in tabular form in the Wireless Location System for use in correcting subsequent location processing.

20 Performance Monitoring

The Wireless Location System uses methods similar to calibration for performance monitoring on a regular and ongoing basis. These methods are depicted in the flowcharts of Figure 2K and 2L. Two methods of performance monitoring are used: fixed phones and drive testing of surveyed points. The fixed phone method comprises the
25 following steps (see Figure 2K):

- standard wireless transmitters are permanently placed at various points within the coverage area of the Wireless Location System (these are then known as the fixed phones) (step S-30);
- the points at which the fixed phones have been placed are surveyed so that their
30 location is precisely known to within a predetermined distance, for example ten feet (step S-31);
- the surveyed locations are stored in a table in the AP 14 (step S-32);

the fixed phones are permitted to register on the wireless communications system, at the rate and interval set by the wireless communications system for all wireless transmitters on the system (step S-33);

at each registration transmission by a fixed phone, the Wireless Location System

5 locates the fixed phone using normal location processing (as with the calibration transmitters, the Wireless Location System can identify a transmission as being from a fixed phone by storing the identities in a table) (step S-34);

the Wireless Location System computes an error between the calculated location determined by the location processing and the stored location determined by

10 survey (step S-35);

the location, the error value, and other measured parameters are stored along with a time stamp in a database in the AP 14 (step S-36);

the AP 14 monitors the instant error and other measured parameters (collectively referred to as an extended location record) and additionally computes various

15 statistical values of the error(s) and other measured parameters (step S-37); and

if any of the error or other values exceed a pre-determined threshold or a historical statistical value, either instantaneously or after performing statistical filtering over a prescribed number of location estimates, the AP 14 signals an alarm to the operator of the Wireless Location System (step S-38).

20

The extended location record includes a large number of measured parameters usefully for analyzing the instant and historical performance of the Wireless Location System. These parameters include: the RF channel used by the wireless transmitter, the antenna port(s) used by the Wireless Location System to demodulate the wireless transmission,

25 the antenna ports from which the Wireless Location System requested RF data, the peak, average, and variance in power of the transmission over the interval used for location processing, the SCS 10 and antenna port chosen as the reference for location processing, the correlation value from the cross-spectra correlation between every other SCS 10 and antenna used in location processing and the reference SCS 10 and antenna, the delay

30 value for each baseline, the multipath mitigation parameters, and the residual values remaining after the multipath mitigation calculations. Any of these measured parameters can be monitored by the Wireless Location System for the purpose of determining how

the Wireless Location System is performing. One example of the type of monitoring performed by the Wireless Location System may be the variance between the instant value of the correlation on a baseline and the historical range of the correlation value. Another may be the variance between the instant value of the received power at a particular antenna and the historical range of the received power. Many other statistical values can be calculated and this list is not exhaustive.

The number of fixed phones placed into the coverage area of the Wireless Location System can be determined based upon the density of the cell sites, the difficulty of the terrain, and the historical ease with which wireless communications systems have performed in the area. Typically the ratio is about one fixed phone for every six cell sites, however in some areas a ratio of one to one may be required. The fixed phones provide a continuous means to monitor the performance of the Wireless Location System, as well as the monitor any changes in the frequency plan that the carrier may have made. Many times, changes in the frequency plan will cause a variation in the performance of the Wireless Location System and the performance monitoring of the fixed phones provide an immediate indication to the Wireless Location System operator.

Drive testing of surveyed points is very similar to the fixed phone monitoring. Fixed phones typically can only be located indoors where access to power is available (i.e. the phones must be continuously powered on to be effective). To obtain a more complete measurement of the performance of the location performance, drive testing of outdoor test points is also performed. Referring to Figure 2L, as with the fixed phones, prescribed test points throughout the coverage area of the Wireless Location System are surveyed to within ten feet (step S-40). Each test point is assigned a code, wherein the code consists of either a "*" or a "#", followed by a sequence number (step S-41). For example, "*1001" through "*1099" may be a sequence of 99 codes used for test points. These codes should be sequences, that when dialed, are meaningless to the wireless communications system (i.e. the codes do not cause a feature or other translation to occur in the MSC, except for an intercept message). The AP 14 stores the code for each test point along with the surveyed location (step S-42). Subsequent to these initial steps, any wireless transmitter dialing any of the codes will be triggered and located using normal

location processing (steps S-43 and S-44). The Wireless Location System automatically computes an error between the calculated location determined by the location processing and the stored location determined by survey, and the location and the error value are stored along with a time stamp in a database in the AP 14 (steps S-45 and S-46). The AP
5 14 monitors the instant error, as well as various historical statistical values of the error. If the error values exceed a pre-determined threshold or a historical statistical value, either instantaneously or after performing statistical filtering over a prescribed number of location estimates, the AP 14 signals an alarm to the operator of the Wireless Location System (step S-47).

10

TDOA Location Processor (TLP)

The TLP 12, depicted in Figures 1, 1A and 3, is a centralized digital signal processing system that manages many aspects of the Wireless Location System, especially the SCS's 10, and provides control over the location processing. Because
15 location processing is DSP intensive, one of the major advantages of the TLP 12 is that the DSP resources can be shared among location processing initiated by transmissions at any of the SCS's 10 in a Wireless Location System. That is, the additional cost of DSP's at the SCS's 10 is reduced by having the resource centrally available. As shown in Figure 3, there are three major components of the TLP 12: DSP modules 12-1, T1/E1
20 communications modules 12-2 and a controller module 12-3.

The T1/E1 communications modules 12-2 provide the communications interface to the SCS's 10 (T1 and E1 are standard communications speeds available throughout the world). Each SCS 10 communicates to a TLP 12 using one or more DS0's (which are
25 typically 56Kbps or 64 Kbps). Each SCS 10 typically connects to a fractional T1 or E1 circuit, using, e.g., a drop and insert unit or channel bank at the cell site. Frequently, this circuit is shared with the base station, which communicates with the MSC. At a central site, the DS0's assigned to the base station are separated from the DS0's assigned to the SCS's 10. This is typically accomplished external to the TLP 12 using a digital access
30 and control system (DACS) 13A that not only separates the DS0's but also grooms the DS0's from multiple SCS's 10 onto full T1 or E1 circuits. These circuits then connect from the DACS 13A to the DACS 13B and then to the T1/E1 communications module

on the TLP 12. Each T1/E1 communications module contains sufficient digital memory to buffer packets of data to and from each SCS 10 communicating with the module. A single TLP chassis may support one or more T1/E1 communications modules.

- 5 The DSP modules 12-1 provide a pooled resource for location processing. A single module may typically contain two to eight digital signal processors, each of which are equally available for location processing. Two types of location processing are supported: central based and station based, which are described in further detail below. The TLP controller 12-3 manages the DSP module(s) 12-1 to obtain optimal throughput.
- 10 Each DSP module contains sufficient digital memory to store all of the data necessary for location processing. A DSP is not engaged until all of the data necessary to begin location processing has been moved from each of the involved SCS's 10 to the digital memory on the DSP module. Only then is a DSP given the specific task to locate a specific wireless transmitter. Using this technique, the DSP's , which are an expensive
- 15 resource, are never kept waiting. A single TLP chassis may support one or more DSP modules.

- The controller module 12-3 provides the real time management of all location processing within the Wireless Location System. The AP 14 is the top-level management entity
- 20 within the Wireless Location System, however its database architecture is not sufficiently fast to conduct the real time decision making when transmissions occur. The controller module 12-3 receives messages from the SCS's 10, including: status, spectral energy in various channels for various antennas, demodulated messages, and diagnostics. This enables the controller to continuously determine events occurring in the Wireless
- 25 Location System, as well as to send commands to take certain actions. When a controller module receives demodulated messages from SCS's 10, the controller module decides whether location processing is required for a particular wireless transmission. The controller module 12-3 also determines which SCS's 10 and antennas to use in location processing, including whether to use central based or station based location processing.
- 30 The controller module commands SCS's 10 to return the necessary data, and commands the communications modules and DSP modules to sequentially perform their necessary roles in location processing. These steps are described below in further detail.

The controller module 12-3 maintains a table known as the Signal of Interest Table (SOIT). This table contains all of the criteria that may be used to trigger location processing on a particular wireless transmission. The criteria may include, for example, the Mobile Identity Number, the Mobile Station ID, the Electronic Serial Number, dialed digits, System ID, RF channel number, cell site number or sector number, type of transmission, and other types of data elements. Some of the trigger events may have higher or lower priority levels associated with them for use in determining the order of processing. Higher priority location triggers will always be processing before lower priority location triggers. However, a lower priority trigger that has already begun location processing will complete the processing before being assigned to a higher priority task. The master Tasking List for the Wireless Location System is maintained on the AP 14, and copies of the Tasking List are automatically downloaded to the Signal of Interest Table in each TLP 12 in the Wireless Location System. The full Signal of Interest Table is downloaded to a TLP 12 when the TLP 12 is reset or first starts. Subsequent to those two events, only changes are downloaded from the AP 14 to each TLP 12 to conserve communications bandwidth. The TLP 12 to AP 14 communications protocol preferably contains sufficient redundancy and error checking to prevent incorrect data from ever being entered into the Signal of Interest Table. When the AP 14 and TLP 12 periodically have spare processing capacity available, the AP 14 reconfirms entries in the Signal of Interest Table to ensure that all Signal of Interest Table entries in the Wireless Location System are in full synchronization.

Each TLP chassis has a maximum capacity associated with the chassis. For example, a single TLP chassis may only have sufficient capacity to support between 48 and 60 SCS's 10. When a wireless communications system is larger than the capacity of a single TLP chassis, multiple TLP chassis are connected together using Ethernet networking. The controller module 12-3 is responsible for inter-TLP communications and networking, and communicates with the controller modules in other TLP chassis and with Application Processors 14 over the Ethernet network. Inter-TLP communications is required when location processing requires the use of SCS's 10 that are connected to different TLP chassis. Location processing for each wireless transmission is assigned to a

single DSP module in a single TLP chassis. The controller modules 12-3 in TLP chassis select the DSP module on which to perform location processing, and then route all of the RF data used in location processing to that DSP module. If RF data is required from the SCS's 10 connected to more than one TLP 12, then the controller modules in all
5 necessary TLP chassis communicate to move the RF data from all necessary SCS's 10 to their respective connected TLP's 12 and then to the DSP module and TLP chassis assigned to the location processing. The controller module supports two fully independent Ethernet networks for redundancy. A break or failure in any one network causes the affected TLP's 12 to immediately shift all communications to the other
10 network.

The controller modules 12-3 maintain a complete network map of the Wireless Location System, including the SCS's 10 associated with each TLP chassis. The network map is a table stored in the controller module containing a list of the candidate SCS/antennas that
15 may be used in location processing, and various parameters associated with each of the SCS/antennas. The structure of an exemplary network map is depicted in Figure 3A. There is a separate entry in the table for each antenna connected to an SCS 10. When a wireless transmission occurs in an area that is covered by SCS's 10 communicating with more than one TLP chassis, the controller modules in the involved TLP chassis
20 determine which TLP chassis will be the "master" TLP chassis for the purpose of managing location processing. Typically, the TLP chassis associated with the SCS 10 that has the primary channel assignment for the wireless transmission is assigned to be the master. However, another TLP chassis may be assigned instead if that TLP temporarily has no DSP resources available for location processing, or if most of the
25 SCS's 10 involved in location processing are connected to another TLP chassis and the controller modules are minimizing inter-TLP communications. This decision making process is fully dynamic, but is assisted by tables in the TLP 12 that pre-determine the preferred TLP chassis for every primary channel assignment. The tables are created by the operator of the Wireless Location System, and programmed using the Network
30 Operations Console.

The networking described herein functions for both TLP chassis associated with the same wireless carrier, as well as for chassis that overlap or border the coverage area between two wireless carriers. Thus it is possible for a TLP 12 belonging to a first wireless carrier to be networked and therefore receive RF data from a TLP 12 (and the SCS's 10 associated with that TLP 12) belonging to a second wireless carrier. This networking is particularly valuable in rural areas, wherein the performance of the Wireless Location System can be enhanced by deploying SCS's 10 at cell sites of multiple wireless carriers. Since in many cases wireless carriers do not colocate cell sites, this feature enables the Wireless Location System to access more geographically diverse antennas than might be available if the Wireless Location System used only the cell sites from a single wireless carrier. As described below, the proper selection and use of antennas for location processing can enhance the performance of the Wireless Location System.

The controller module 12-3 passes many messages, including location records, to the AP 14, many of which are described below. Usually, however, demodulated data is not passed from the TLP 12 to the AP 14. If, however, the TLP 12 receives demodulated data from a particular wireless transmitter and the TLP 12 identifies the wireless transmitter as being a registered customer of a second wireless carrier in a different coverage area, the TLP 12 may pass the demodulated data to the first (serving) AP 14A. This will enable the first AP 14A to communicate with a second AP 14B associated with the second wireless carrier, and determine whether the particular wireless transmitter has registered for any type of location services. If so, the second AP 14B may instruct the first AP 14A to place the identity of the particular wireless transmitter into the Signal of Interest Table so that the particular wireless transmitter will be located for as long as the particular wireless transmitter is in the coverage area of the first Wireless Location System associated with the first AP 14A. When the first Wireless Location System has detected that the particular wireless transmitter has not registered in a time period exceeding a pre-determined threshold, the first AP 14A may instruct the second AP 14B that the identity of the particular wireless transmitter is being removed from the Signal of Interest Table for the reason of no longer being present in the coverage area associated with the first AP 14A.

Diagnostic Port

The TLP 12 supports a diagnostic port that is highly useful in the operation and diagnosis of problems within the Wireless Location System. This diagnostic port can be
5 accessed either locally at a TLP 12 or remotely over the Ethernet network connecting the TLP's 12 to the AP's. The diagnostic port enables an operator to write to a file all of the demodulation and RF data received from the SCS's 10, as well as the intermediate and final results of all location processing. This data is erased from the TLP 12 after processing a location estimate, and therefore the diagnostic port provides the means to
10 save the data for later post-processing and analysis. The inventor's experience in operating large scale wireless location systems is that a very small number of location estimates can occasionally have very large errors, and these large errors can dominate the overall operating statistics of the Wireless Location System over any measurement period. Therefore, it is important to provide the operator with a set of tools that enable
15 the Wireless Location System to detect and trap the cause of the very large errors to diagnose and mitigate those errors. The diagnostic port can be set to save the above information for all location estimates, for location estimates from particular wireless transmitters or at particular test points, or for location estimates that meet a certain criteria. For example, for fixed phones or drive testing of surveyed points, the diagnostic
20 port can determine the error in the location estimate in real time and then write the above described information only for those location estimates whose error exceeds a predetermined threshold. The diagnostic port determines the error in real time by storing the surveyed latitude, longitude coordinate of each fixed phone and drive test point in a table, and then calculating a radial error when a location estimate for the corresponding
25 test point is made.

Redundancy

The TLP's 12 implement redundancy using several inventive techniques, allowing the Wireless Location System to support an M plus N redundancy method. M
30 plus N redundancy means that N redundant (or standby) TLP chassis are used to provide full redundant backup to M online TLP chassis. For example, M may be ten and N may be two.

First, the controller modules in different TLP chassis continuously exchange status and “heartbeat” messages at pre-determined time intervals between themselves and with every AP 14 assigned to monitor the TLP chassis. Thus, every controller module has continuous and full status of every other controller module in the Wireless Location System. The controller modules in different TLP chassis periodically select one controller module in one TLP 12 to be the master controller for a group of TLP chassis. The master controller may decide to place a first TLP chassis into off-line status if the first TLP 12A reports a failed or degraded condition in its status message, or if the first TLP 12A fails to report any status or heartbeat messages within its assigned and pre-determined time. If the master controller places a first TLP 12A into off-line status, the master controller may assign a second TLP 12B to perform a redundant switchover and assume the tasks of the off-line first TLP 12A. The second TLP 12B is automatically sent the configuration that had been loaded into the first TLP 12A; this configuration may be downloaded from either the master controller or from an AP 14 connected to the TLP’s 12. The master controller may be a controller module on any one of the TLP’s 12 that is not in off-line status, however there is a preference that the master controller be a controller module in a stand-by TLP 12. When the master controller is the controller module in a stand-by TLP 12, the time required to detect a failed first TLP 12A, place the first TLP 12A into off-line status, and then perform a redundant switchover can be accelerated.

Second, all of the T1 or E1 communications between the SCS’s 10 and each of the TLP T1/E1 communications modules 12-2 are preferably routed through a high-reliability DACS that is dedicated to redundancy control. The DACS 13B is connected to every groomed T1/E1 circuit containing DS0’s from SCS’s 10 and is also connected to every T1/E1 communications module 12-2 of every TLP 12. Every controller module at every TLP 12 contains a map of the DACS 13B that describes the DACS’ connection list and port assignments. This DACS 13B is connected to the Ethernet network described above and can be controlled by any of the controller modules 12-3 at any of the TLP’s 12. When a second TLP 12 is placed into off-line status by a master controller, the master controller sends commands to the DACS 13B to switch the groomed T1/E1 circuit

communicating with the first TLP 12A to a second TLP 12B which had been in standby status. At the same time, the AP 14 downloads the complete configuration file that was being used by the second (and now off-line) TLP 12B to the third (and now online) TLP 12C. The time from the first detection of a failed first TLP chassis to the complete
5 switch-over and assumption of processing responsibilities by a third TLP chassis is typically less than few seconds. In many cases, no RF data is lost by the SCS's 10 associated with the failed first TLP chassis, and location processing can continue without interruption. At the time of a TLP fail-over when a first TLP 12A is placed into off-line status, the NOC 16 creates an alert to notify the Wireless Location System operator that
10 the event has occurred.

Third, each TLP chassis contains redundant power supplies, fans, and other components. A TLP chassis can also support multiple DSP modules, so that the failure of a single DSP module or even a single DSP on a DSP module reduces the overall amount of
15 processing resources available but does not cause the failure of the TLP chassis. In all of the cases described in this paragraph, the failed component of the TLP 12 can be replaced without placing the entire TLP chassis into off-line status. For example, if a single power supply fails, the redundant power supply has sufficient capacity to singly support the load of the chassis. The failed power supply contains the necessary circuitry
20 to remove itself from the load of the chassis and not cause further degradation in the chassis. Similarly, a failed DSP module can also remove itself from the active portions of the chassis, so as to not cause a failure of the backplane or other modules. This enables the remainder of the chassis, including the second DSP module, to continue to function normally. Of course, the total processing throughput of the chassis is reduced but a total
25 failure is avoided.

Application Processor (AP) 14

The AP 14 is a centralized database system, comprising a number of software processes that manage the entire Wireless Location System, provide interfaces to
30 external users and applications, store location records and configurations, and support various application-related functionality. The AP 14 uses a commercial hardware platform that is sized to match the throughput of the Wireless Location System. The AP

14 also uses a commercial relational database system (RDBMS), which has been significantly customized to provide the functionality described herein. While the SCS 10 and TLP 12 preferably operate together on a purely real time basis to determine location and create location records, the AP 14 can operate on both a real time basis to store and forward location records and a non-real time basis to post-process location records and provide access and reporting over time. The ability to store, retrieve, and post-process location records for various types of system and application analysis has proven to be a powerful advantage of the present invention. The main collection of software processes is known as the ApCore, which is shown in Figure 4 and includes the following functions:

The AP Performance Guardian (ApPerfGuard) is a dedicated software process that is responsible for starting, stopping, and monitoring most other ApCore processes as well as ApCore communications with the NOC 16. Upon receiving a configuration update command from the NOC, ApPerfGuard updates the database and notifies all other processes of the change. ApPerfGuard starts and stops appropriate processes when the NOC directs the ApCore to enter specific run states, and constantly monitors other software processes scheduled to be running to restart them if they have exited or stopping and restarting any process that is no longer properly responding. ApPerfGuard is assigned to one of the highest processing priorities so that this process cannot be blocked by another process that has "run away". ApPerfGuard is also assigned dedicated memory that is not accessible by other software processes to prevent any possible corruption from other software processes.

The AP Dispatcher (ApMnDsptch) is a software process that receives location records from the TLP's 12 and forwards the location records to other processes. This process contains a separate thread for each physical TLP 12 configured in the system, and each thread receives location records from that TLP 12. For system reliability, the ApCore maintains a list containing the last location record sequence number received from each TLP 12, and sends this sequence number to the TLP 12 upon initial connection. Thereafter, the AP 14 and the TLP 12 maintain a protocol whereby the TLP 12 sends

each location record with a unique identifier. ApMnDsptch forwards location records to multiple processes, including Ap911, ApDbSend, ApDbRecvLoc, and ApDbFileRecv.

- The AP Tasking Process (ApDbSend) controls the Tasking List within the Wireless
- 5 Location System. The Tasking List is the master list of all of the trigger criteria that determines which wireless transmitters will be located, which applications created the criteria, and which applications can receive location record information. The ApDbSend process contains a separate thread for each TLP 12, over which the ApDbSend synchronizes the Tasking List with the Signal of Interest Table on each TLP 12.
- 10 ApDbSend does not send application information to the Signal of Interest Table, only the trigger criteria. Thus the TLP 12 does not know why a wireless transmitter must be located. The Tasking List allows wireless transmitters to be located based upon Mobile Identity Number (MIN), Mobile Station Identifier (MSID), Electronic Serial Number (ESN) and other identity numbers, dialed sequences of characters and / or digits, home
- 15 System ID (SID), originating cell site and sector, originating RF channel, or message type. The Tasking List allows multiple applications to receive location records from the same wireless transmitter. Thus, a single location record from a wireless transmitter that has dialed "911" can be sent, for example, to a 911 PSAP, a fleet management application, a traffic management application, and to an RF optimization application.
- 20

- The Tasking List also contains a variety of flags and field for each trigger criteria, some of which are described elsewhere in this specification. One flag, for example, specifies the maximum time limit before which the Wireless Location System must provide a rough or final estimate of the wireless transmitter. Another flag allows location
- 25 processing to be disabled for a particular trigger criteria such as the identity of the wireless transmitter. Another field contains the authentication required to make changes to the criteria for a particular trigger; authentication enables the operator of the Wireless Location System to specify which applications are authorized to add, delete, or make changes to any trigger criteria and associated fields or flags. Another field contains the
- 30 Location Grade of Service associated with the trigger criteria; Grade of Service indicates to the Wireless Location System the accuracy level and priority level desired for the location processing associated with a particular trigger criteria. For example, some

applications may be satisfied with a rough location estimate (perhaps for a reduced location processing fee), while other applications may be satisfied with low priority processing that is not guaranteed to complete for any given transmission (and which may be pre-empted for high priority processing tasks). The Wireless Location System also
5 includes means to support the use of wildcards for trigger criteria in the Tasking List. For example, a trigger criteria can be entered as "MIN = 215555****". This will cause the Wireless Location System to trigger location processing for any wireless transmitter whose MIN begins with the six digits 215555 and ends with any following four digits. The wildcard characters can be placed into any position in a trigger criteria. This feature
10 can save on the number of memory locations required in the Tasking List and Signal of Interest Table by grouping blocks of related wireless transmitters together.

ApDbSend also supports dynamic tasking. For example, the MIN, ESN, MSID, or other identity of any wireless transmitter that has dialed "911" will automatically be placed
15 onto the Tasking List by ApDbSend for one hour. Thus, any further transmissions by the wireless transmitter that dialed "911" will also be located in case of further emergency. For example, if a PSAP calls back a wireless transmitter that had dialed "911" within the last hour, the Wireless Location System will trigger on the page response message from the wireless transmitter, and can make this new location record available to the PSAP.
20 This dynamic tasking can be set for any interval of time after an initiation event, and for any type of trigger criteria. The ApDbSend process is also a server for receiving tasking requests from other applications. These applications, such as fleet management, can send tasking requests via a socket connection, for example. These applications can either place or remove trigger criteria. ApDbSend conducts an authentication process with each
25 application to verify that that the application has been authorized to place or remove trigger criteria, and each application can only change trigger criteria related to that application.

The AP 911 Process (Ap911) manages each interface between the Wireless Location
30 System and E9-1-1 network elements, such as tandem switches, selective routers, ALI databases and/or PSAPs. The Ap911 process contains a separate thread for each connection to a E9-1-1 network element, and can support more than one thread to each

network element. The Ap911 process can simultaneously operate in many modes based upon user configuration, and as described herein. The timely processing of E9-1-1 location records is one of the highest processing priorities in the AP 14, and therefore the Ap911 executes entirely out of random access memory (RAM) to avoid the delay
5 associated with first storing and then retrieving a location record from any type of disk. When ApMnDsptch forwards a location record to Ap911, Ap911 immediately makes a routing determination and forwards the location record over the appropriate interface to a E9-1-1 network element. A separate process, operating in parallel, records the location record into the AP 14 database.

10

The AP 14, through the Ap911 process and other processes, supports two modes of providing location records to applications, including E9-1-1: "push" and "pull" modes. Applications requesting push mode receive a location record as soon as it is available from the AP 14. This mode is especially effective for E9-1-1 which has a very time
15 critical need for location records, since E9-1-1 networks must route wireless 9-1-1 calls to the correct PSAP within a few seconds after a wireless caller has dialed "911". Applications requesting pull mode do not automatically receive location records, but rather must send a query to the AP 14 regarding a particular wireless transmitter in order to receive the last, or any other location record, about the wireless transmitter. The query
20 from the application can specify the last location record, a series of location records, or all location records meeting a specific time or other criteria, such as type of transmission. An example of the use of pull mode in the case of a "911" call is the E9-1-1 network first receiving the voice portion of the "911" call and then querying the AP 14 to receive the location record associated with that call.

25

When the Ap911 process is connected to many E9-1-1 networks elements, Ap911 must determine to which E9-1-1 network element to push the location record (assuming that "push" mode has been selected). The AP 14 makes this determination using a dynamic routing table. The dynamic routing table is used to divide a geographic region into cells.
30 Each cell, or entry, in the dynamic routing table contains the routing instructions for that cell. It is well known that one minute of latitude is 6083 feet, which is about 365 feet per millidegree. Additionally, one minute of longitude is cosine(latitude) times 6083 feet,

which for the Philadelphia area is about 4659 feet, or about 280 feet per millidegree. A table of size one thousand by one thousand, or one million cells, can contain the routing instructions for an area that is about 69 miles by 53 miles, which is larger than the area of Philadelphia in this example, and each cell could contain a geographic area of 365 feet
5 by 280 feet. The number of bits allocated to each entry in the table must only be enough to support the maximum number of routing possibilities. For example, if the total number of routing possibilities is sixteen or less, then the memory for the dynamic routing table is one million times four bits, or one-half megabyte. Using this scheme, an area the size of Pennsylvania could be contained in a table of approximately twenty megabytes or
10 less, with ample routing possibilities available. Given the relatively inexpensive cost of memory, this inventive dynamic routing table provides the AP 14 with a means to quickly push the location records for "911" calls only to the appropriate E9-1-1 network element.

15 The AP 14 allows each entry in dynamic routing to be populated using manual or automated means. Using the automated means, for example, an electronic map application can create a polygon definition of the coverage area of a specific E9-1-1 network element, such as a PSAP. The polygon definition is then translated into a list of latitude, longitude points contained within the polygon. The dynamic routing table cell
20 corresponding to each latitude, longitude point is then given the routing instruction for that E9-1-1 network element that is responsible for that geographic polygon.

When the Ap911 process receives a "911" location record for a specific wireless transmitter, Ap911 converts the latitude, longitude into the address of a specific cell in
25 the dynamic routing table. Ap911 then queries the cell to determine the routing instructions, which may be push or pull mode and the identity of the E9-1-1 network element responsible for serving the geographic area in which the "911" call occurred. If push mode has been selected, then Ap911 automatically pushes the location record to that E9-1-1 network element. If pull mode has been selected, then Ap911 places the
30 location record into a circular table of "911" location records and awaits a query.

The dynamic routing means described above entails the use of a geographically defined database that may be applied to other applications in addition to 911, and is therefore supported by other processes in addition to Ap911. For example, the AP 14 can automatically determine the billing zone from which a wireless call was placed for a

5 Location Sensitive Billing application. In addition, the AP 14 may automatically send an alert when a particular wireless transmitter has entered or exited a prescribed geographic area defined by an application. The use of particular geographic databases, dynamic routing actions, any other location triggered actions are defined in the fields and flags associated with each trigger criteria. The Wireless Location System includes means to

10 easily manage these geographically defined databases using an electronic map that can create polygons encompassing a prescribed geographic area. The Wireless Location System extracts from the electronic map a table of latitude, longitude points contained with the polygon. Each application can use its own set of polygons, and can define a set of actions to be taken when a location record for a triggered wireless transmission is

15 contained within each polygon in the set.

The AP Database Receive Process (ApDbRecvLoc) receives all location records from ApMnDsptch via shared memory, and places the location records into the AP location database. ApDbRecvLoc starts ten threads that each retrieve location records from

20 shared memory, validate each record before inserting the records into the database, and then inserts the records into the correct location record partition in the database. To preserve integrity, location records with any type of error are not written into the location record database but are instead placed into an error file that can be reviewed by the Wireless Location System operator and then manually entered into the database after

25 error resolution. If the location database has failed or has been placed into off-line status, location records are written to a flat file where they can be later processed by ApDbFileRecv.

The AP File Receive Process (ApDbFileRecv) reads flat files containing location records

30 and inserts the records into the location database. Flat files are a safe mechanism used by the AP 14 to completely preserve the integrity of the AP 14 in all cases except a complete failure of the hard disk drives. There are several different types of flat files read

by ApDbFileRecv, including Database Down, Synchronization, Overflow, and Fixed Error. Database Down flat files are written by the ApDbRecvLoc process if the location database is temporarily inaccessible; this file allows the AP 14 to ensure that location records are preserved during the occurrence of this type of problem. Synchronization flat files are written by the ApLocSync process (described below) when transferring location records between pairs of redundant AP systems. Overflow flat files are written by ApMnDsptch when location records are arriving into the AP 14 at a rate faster than ApDbRecvLoc can process and insert the records into the location database. This may occur during very high peak rate periods. The overflow files prevent any records from being lost during peak periods. The Fixed Error flat files contain location records that had errors but have now been fixed, and can now be inserted into the location database.

Because the AP 14 has a critical centralized role in the Wireless Location System, the AP 14 architecture has been designed to be fully redundant. A redundant AP 14 system includes fully redundant hardware platforms, fully redundant RDBMS, redundant disk drives, and redundant networks to each other, the TLP's 12, the NOC's 16, and external applications. The software architecture of the AP 14 has also been designed to support fault tolerant redundancy. The following examples illustrate functionality supported by the redundant AP's. Each TLP 12 sends location records to both the primary and the redundant AP 14 when both AP's are in an online state. Only the primary AP 14 will process incoming tasking requests, and only the primary AP 14 will accept configuration change requests from the NOC 16. The primary AP 14 then synchronizes the redundant AP 14 under careful control. Both the primary and redundant AP's will accept basic startup and shutdown commands from the NOC. Both AP's constantly monitor their own system parameters and application health and monitor the corresponding parameters for the other AP 14, and then decide which AP 14 will be primary and which will be redundant based upon a composite score. This composite score is determined by compiling errors reported by various processes to a shared memory area, and monitoring swap space and disk space. There are several processes dedicated to supporting redundancy.

The AP Location Synchronization Process (ApLocSync) runs on each AP 14 and detects the need to synchronize location records between AP's, and then creates "sync records" that list the location records that need to be transferred from one AP 14 to another AP 14. The location records are then transferred between AP's using a socket connection.

- 5 ApLocSync compares the location record partitions and the location record sequence numbers stored in each location database. Normally, if both the primary and redundant AP 14 are operating properly, synchronization is not needed because both AP's are receiving location records simultaneously from the TLP's 12. However, if one AP 14 fails or is placed in an off-line mode, then synchronization will later be required.
- 10 ApLocSync is notified whenever ApMnDsptch connects to a TLP 12 so it can determine whether synchronization is required.

The AP Tasking Synchronization Process (ApTaskSync) runs on each AP 14 and synchronizes the tasking information between the primary AP 14 and the redundant AP

15 14. ApTaskSync on the primary AP 14 receives tasking information from ApDbSend, and then sends the tasking information to the ApTaskSync process on the redundant AP 14. If the primary AP 14 were to fail before ApTaskSync had completed replicating tasks, then ApTaskSync will perform a complete tasking database synchronization when the failed AP 14 is placed back into an online state.

20

The AP Configuration Synchronization Process (ApConfigSync) runs on each AP 14 and synchronizes the configuration information between the primary AP 14 and the redundant AP 14. ApConfigSync uses a RDBMS replication facility. The configuration information includes all information needed by the SCS's 10, TLP's 12, and AP's 14 for

25 proper operation of the Wireless Location System in a wireless carrier's network.

- In addition to the core functions described above, the AP 14 also supports a large number of processes, functions, and interfaces useful in the operation of the Wireless Location System, as well as useful for various applications that desire location information. While
- 30 the processes, functions, and interfaces described herein are in this section pertaining to the AP 14, the implementation of many of these processes, functions, and interfaces

permeates the entire Wireless Location System and therefore their inventive value should be not read as being limited only to the AP 14.

Roaming

- 5 The AP 14 supports “roaming” between wireless location systems located in different cities or operated by different wireless carriers. If a first wireless transmitter has subscribed to an application on a first Wireless Location System, and therefore has an entry in the Tasking List in the first AP 14 in the first Wireless Location System, then the first wireless transmitter may also subscribe to roaming. Each AP 14 and TLP 12 in each
- 10 Wireless Location System contains a table in which a list of valid “home” subscriber identities is maintained. The list is typically a range, and for example, for current cellular telephones, the range can be determined by the NPA/NXX codes (or area code and exchange) associated with the MIN or MSID of cellular telephones. When a wireless transmitter meeting the “home” criteria makes a transmission, a TLP 12 receives
- 15 demodulated data from one or more SCS’s 10 and checks the trigger information in the Signal of Interest Table . If any trigger criterion is met, the location processing begins on that transmission; otherwise, the transmission is not processed by the Wireless Location System.
- 20 When a first wireless transmitter not meeting the “home” criterion makes a transmission in a second Wireless Location System, the second TLP 12 in the second Wireless Location System checks the Signal of Interest Table for a trigger. One of three actions then occurs: (i) if the transmission meets an already existing criteria in the Signal of Interest Table , the transmitter is located and the location record is forwarded from the
- 25 second AP 14 in the second Wireless Location System to the first AP 14 in the first Wireless Location System; (ii) if the first wireless transmitter has a “roamer” entry in the Signal of Interest Table indicating that the first wireless transmitter has “registered” in the second Wireless Location System but has no trigger criteria, then the transmission is not processed by the second Wireless Location System and the expiration timestamp is
- 30 adjusted as described below; (iii) if the first wireless transmitter has no “roamer” entry and therefore has not “registered”, then the demodulated data is passed from the TLP 12 to the second AP 14.

In the third case above, the second AP 14 uses the identity of the first wireless transmitter to identify the first AP 14 in the first Wireless Location System as the “home” Wireless Location System of the first wireless transmitter. The second AP 14 in
5 the second Wireless Location System sends a query to the first AP 14 in the first Wireless Location System to determine whether the first wireless transmitter has subscribed to any location application and therefore has any trigger criteria in the Tasking List of the first AP 14. If a trigger is present in the first AP 14, the trigger criteria, along with any associated fields and flags, is sent from the first AP 14 to the
10 second AP 14 and entered in the Tasking List and the Signal of Interest Table as a “roamer” entry with trigger criteria. If the first AP 14 responds to the second AP 14 indicating that the first wireless transmitter has no trigger criteria, then the second AP 14 “registers” the first wireless transmitter in the Tasking List and the Signal of Interest Table as a “roamer” with no trigger criteria. Thus both current and future transmissions
15 from the first wireless transmitter can be positively identified by the TLP 12 in the second Wireless Location System as being registered without trigger criteria, and the second AP 14 is not required to make additional queries to the first AP 14.

When the second AP 14 registers the first wireless transmitter with a roamer entry in the
20 Tasking List and the Signal of Interest Table with or without trigger criteria, the roamer entry is assigned an expiration timestamp. The expiration timestamp is set to the current time plus a predetermined first interval. Every time the first wireless transmitter makes a transmission, the expiration timestamp of the roamer entry in the Tasking List and the Signal of Interest Table is adjusted to the current time of the most recent transmission
25 plus the predetermined first interval. If the first wireless transmitter makes no further transmissions prior to the expiration timestamp of its roamer entry, then the roamer entry is automatically deleted. If, subsequent to the deletion, the first wireless transmitter makes another transmission, then the process of registering occurs again.

30 The first AP 14 and second AP 14 maintain communications over a wide area network. The network may be based upon TCP/IP or upon a protocol similar to the most recent version of IS-41. Each AP 14 in communications with other AP’s in other wireless

location systems maintains a table that provides the identity of each AP 14 and Wireless Location System corresponding to each valid range of identities of wireless transmitters.

Multiple Pass Location Records

- 5 Certain applications may require a very fast estimate of the general location of a wireless transmitter, followed by a more accurate estimate of the location that can be sent subsequently. This can be valuable, for example, for E9-1-1 systems that handle wireless calls and must make a call routing decision very quickly, but can wait a little longer for a more exact location to be displayed upon the E9-1-1 call-taker's electronic map terminal.
- 10 The Wireless Location System supports these applications with an inventive multiple pass location processing mode, described later. The AP 14 supports this mode with multiple pass location records. For certain entries, the Tasking List in the AP 14 contains a flag indicating the maximum time limit before which a particular application must receive a rough estimate of location, and a second maximum time limit in which a
- 15 particular application must receive a final location estimate. For these certain applications, the AP 14 includes a flag in the location record indicating the status of the location estimate contained in the record, which may, for example, be set to first pass estimate (i.e. rough) or final pass estimate. The Wireless Location System will generally determine the best location estimate within the time limit set by the application, that is
- 20 the Wireless Location System will process the most amount of RF data that can be supported in the time limit. Given that any particular wireless transmission can trigger a location record for one or more applications, the Wireless Location System supports multiple modes simultaneously. For example, a wireless transmitter with a particular MIN can dial "911". This may trigger a two-pass location record for the E9-1-1
- 25 application, but a single pass location record for a fleet management application that is monitoring that particular MIN. This can be extended to any number of applications.

Multiple Demodulation and Triggers

- In wireless communications systems in urban or dense suburban areas,
- 30 frequencies or channels can be re-used several times within relatively close distances. Since the Wireless Location System is capable of independently detecting and demodulating wireless transmissions without the aid of the wireless communications

system, a single wireless transmission can frequently be detected and successfully demodulated at multiple SCS's 10 within the Wireless Location System. This can happen both intentionally and unintentionally. An unintentional occurrence is caused by a close frequency re-use, such that a particular wireless transmission can be received above a
5 predetermined threshold at more than one SCS 10, when each SCS 10 believes it is monitoring only transmissions that occur only within the cell site collocated with the SCS 10. An intentional occurrence is caused by programming more than one SCS 10 to detect and demodulate transmissions that occur at a particular cell site and on a particular frequency. As described earlier, this is generally used with adjacent or nearby SCS's 10
10 to provide system demodulation redundancy to further increase the probability that any particular wireless transmission is successfully detected and demodulated.

Either type of event could potentially lead to multiple triggers within the Wireless Location System, causing location processing to be initiated several times for the same
15 transmission. This causes an excess and inefficient use of processing and communications resources. Therefore, the Wireless Location System includes means to detect when the same transmission has been detected and demodulated more than once, and to select the best demodulating SCS 10 as the starting point for location processing. When the Wireless Location System detects and successfully demodulates the same
20 transmission multiple times at multiple SCS/antennas, the Wireless Location System uses the following criteria to select the one demodulating SCS/antenna to use to continue the process of determining whether to trigger and possibly initiate location processing (again, these criteria may be weighted in determining the final decision): (i) an SCS/antenna collocated at the cell site to which a particular frequency has been assigned
25 is preferred over another SCS/antenna, but this preference may be adjusted if there is no operating and on-line SCS/antenna collocated at the cell site to which the particular frequency has been assigned, (ii) SCS/antennas with higher average SNR are preferred over those with lower average SNR, and (iii) SCS/antennas with fewer bit errors in demodulating the transmission are preferred over those with higher bit errors. The
30 weighting applied to each of these preferences may be adjusted by the operator of the Wireless Location System to suit the particular design of each system.

Interface to Wireless Communications System

The Wireless Location System contains means to communicate over an interface to a wireless communications system, such as a mobile switching center (MSC) or mobile positioning controller (MPC). This interface may be based, for example, on a standard secure protocol such as the most recent version of the IS-41 or TCP/IP protocols. The formats, fields, and authentication aspects of these protocols are well known. The Wireless Location System supports a variety of command / response and informational messages over this interface that are designed to aid in the successful detection, demodulation, and triggering of wireless transmissions, as well as providing means to pass location records to the wireless communications system. In particular, this interface provides means for the Wireless Location System to obtain information about which wireless transmitters have been assigned to particular voice channel parameters at particular cell sites. Example messages supported by the Wireless Location System over this interface to the wireless communications system include the following:

Query on MIN / MDN / MSID / IMSI / TMSI Mapping – Certain types of wireless transmitters will transmit their identity in a familiar form that can be dialed over the telephone network. Other types of wireless transmitters transmit an identity that cannot be dialed, but which is translated into a number that can be dialed using a table inside of the wireless communications system. The transmitted identity is permanent in most cases, but can also be temporary. Users of location applications connected to the AP 14 typically prefer to place triggers onto the Tasking List using identities that can be dialed. Identities that can be dialed are typically known as Mobile Directory Numbers (MDN). The other types of identities for which translation may be required includes Mobile Identity Number (MIN), Mobile Subscriber Identity (MSID), International Mobile Subscriber Identity (IMSI), and Temporary Mobile Subscriber Identity (TMSI). If the wireless communications system has enabled the use of encryption for any of the data fields in the messages transmitted by wireless transmitters, the Wireless Location System may also query for encryption information along with the identity information. The Wireless Location System includes means to query the wireless communications system for the alternate identities for a trigger identity that has been placed onto the Tasking List

by a location application, or to query the wireless communications system for alternate identities for an identity that has been demodulated by an SCS 10. Other events can also trigger this type of query. For this type of query, typically the Wireless Location System initiates the command, and the wireless communications system responds.

Query / Command Change on Voice RF Channel Assignment – Many wireless transmissions on voice channels do not contain identity information. Therefore, when the Wireless Location System is triggered to perform location processing on a voice channel transmission, the Wireless Location System queries the wireless communication system to obtain the current voice channel assignment information for the particular transmitter for which the Wireless Location System has been triggered. For an AMPS transmission, for example, the Wireless Location System preferably requires the cell site, sector, and RF channel number currently in use by the wireless transmitter. For a TDMA transmission, for example, the Wireless Location System preferably requires the cell site, sector, RF channel number, and timeslot currently in use by the wireless transmitter. Other information elements that may be needed include long code mask and encryption keys. In general, the Wireless Location System will initiate the command, and the wireless communications system will respond. However, the Wireless Location System will also accept a trigger command from the wireless communications system that contains the information detailed herein.

The timing on this command / response message set is very critical since voice channel handoffs can occur quite frequently in wireless communications systems. That is, the Wireless Location System will locate any wireless transmitter that is transmitting on a particular channel – therefore the Wireless Location System and the wireless communications system must jointly be certain that the identity of the wireless transmitter and the voice channel assignment information are in perfect synchronization. The Wireless Location System uses several means to achieve this objective. The Wireless Location System may, for example, query the voice channel assignment information for a particular wireless transmitter, receive the necessary RF

data, then again query the voice channel assignment information for that same wireless transmitter, and then verify that the status of the wireless transmitter did not change during the time in which the RF data was being collected by the Wireless Location System. Location processing is not required to complete before the second query, since it is only important to verify that the correct RF data was received. The Wireless Location System may also, for example, as part of the first query command the wireless communications system to prevent a handoff from occurring for the particular wireless transmitter during the time period in which the Wireless Location System is receiving the RF data. Then, subsequent to collecting the RF data, the Wireless Location System will again query the voice channel assignment information for that same wireless transmitter, command the wireless communications system to again permit handoffs for the wireless transmitter and then verify that the status of the wireless transmitter did not change during the time in which the RF data was being collected by the Wireless Location System.

For various reasons, either the Wireless Location System or the wireless communications system may prefer that the wireless transmitter be assigned to another voice RF channel prior to performing location processing. Therefore, as part of the command / response sequence, the wireless communications system may instruct the Wireless Location System to temporarily suspend location processing until the wireless communications system has completed a handoff sequence with the wireless transmitter, and the wireless communications system has notified the Wireless Location System that RF data can be received and the voice RF channel upon which the data can be received. Alternatively, the Wireless Location System may determine that the particular voice RF channel which a particular wireless transmitter is currently using is unsuitable for obtaining an acceptable location estimate, and request that the wireless communications system command the wireless transmitter to handoff. Alternatively, the Wireless Location System may request that the wireless communications system command the wireless transmitter to handoff to a series of voice RF channels in sequence in order to perform a series of location estimates, whereby the Wireless Location System can improve upon the accuracy of

the location estimate through the series of handoffs. This method is further described below.

5 The Wireless Location System can also use this command / response message set to query the wireless communications system about the identity of a wireless transmitter that had been using a particular voice channel (and timeslot, etc.) at a particular cell site at a particular time. This enables the Wireless Location System to first perform location processing on transmissions without knowing the identities, and then to later determine the identity of the wireless transmitters making the transmissions and
10 append this information to the location record. This particular inventive feature enables the use of automatic sequential location of voice channel transmissions.

Receive Triggers – The Wireless Location System can receive triggers from the wireless communications system to perform location processing on a voice channel
15 transmission without knowing the identity of the wireless transmitter. This message set bypasses the Tasking List, and does not use the triggering mechanisms within the Wireless Location System. Rather, the wireless communications system alone determines which wireless transmissions to locate, and then sends a command to the Wireless Location System to collect RF data from a particular voice channel at a
20 particular cell site and to perform location processing. The Wireless Location System responds with a confirmation containing a timestamp when the RF data was collected. The Wireless Location System also responds with an appropriate format location record when location processing has completed. Based upon the time of the command to Wireless Location System and the response with the RF data collection
25 timestamp, the wireless communications system determines whether the wireless transmitter status changed subsequent to the command and whether there is a good probability of successful RF data collection.

30 Make Transmit – The Wireless Location System can command the wireless communications system to force a particular wireless transmitter to make a transmission at a particular time, or within a prescribed range of times. The wireless communications system responds with a confirmation and a time or time range in

which to expect the transmission. The types of transmissions that the Wireless Location System can force include, for example, audit responses and page responses. Using this message set, the Wireless Location System can also command the wireless communications system to force the wireless transmitter to transmit using a higher power level setting. In many cases, wireless transmitters will attempt to use the lowest power level settings when transmitting in order to conserve battery life. In order improve the accuracy of the location estimate, the Wireless Location System may prefer that the wireless transmitter use a higher power level setting. The wireless communications system will respond to the Wireless Location System with a confirmation that the higher power level setting will be used and a time or time range in which to expect the transmission.

Delay Wireless Communications System Response to Mobile Access – Some air interface protocols, such as CDMA, use a mechanism in which the wireless transmitter initiates transmissions on a channel, such as an Access Channel, for example, at the lowest or a very low power level setting, and then enters a sequence of steps in which (i) the wireless transmitter makes an access transmission; (ii) the wireless transmitter waits for a response from the wireless communications system; (iii) if no response is received by the wireless transmitter from the wireless communications system within a predetermined time, the wireless transmitter increases its power level setting by a predetermined amount, and then returns to step (i); (iv) if a response is received by the wireless transmitter from the wireless communications system within a predetermined time, the wireless transmitter then enters a normal message exchange. This mechanism is useful to ensure that the wireless transmitter uses only the lowest useful power level setting for transmitting and does not further waste energy or battery life. It is possible, however, that the lowest power level setting at which the wireless transmitter can successfully communicate with the wireless communications system is not sufficient to obtain an acceptable location estimate. Therefore, the Wireless Location System can command the wireless communications system to delay its response to these transmissions by a predetermined time or amount. This delaying action will cause the wireless transmitter to repeat the sequence of steps (i) through (iii) one or more times than

normal with the result that one or more of the access transmissions will be at a higher power level than normal. The higher power level may preferably enable the Wireless Location System to determine a more accurate location estimate. The Wireless Location System may command this type of delaying action for either a particular wireless transmitter, for a particular type of wireless transmission (for example, for all '911' calls), for wireless transmitters that are at a specified range from the base station to which the transmitter is attempting to communicate, or for all wireless transmitters in a particular area.

10 Send Confirmation to Wireless Transmitter – The Wireless Location System does not include means within itself to notify the wireless transmitter of an action because the Wireless Location System cannot transmit; as described earlier the Wireless Location System can only receive transmissions. Therefore, if the Wireless Location System desires to send, for example, a confirmation tone upon the completion of a certain action, the Wireless Location System commands the wireless communications system to transmit a particular message. The message may include, for example, an audible confirmation tone, spoken message, or synthesized message to the wireless transmitter, or a text message sent via a short messaging service or a page. The Wireless Location System receives confirmation from the wireless communications system that the message has been accepted and sent to the wireless transmitter. This command / response message set is important in enabling the Wireless Location System to support certain end-user application functions such as Prohibit Location Processing.

25 Report Location Records – The Wireless Location System automatically reports location records to the wireless communications system for those wireless transmitters tasked to report to the wireless communications system, as well as for those transmissions that the wireless communications system initiated triggers. The Wireless Location System also reports on any historical location record queried by the wireless communications system and which the wireless communications system is authorized to receive.

Monitor Internal Wireless Communications System Interfaces, State Table

In addition to this above interface between the Wireless Location System and the wireless communications system, the Wireless Location System also includes means to monitor existing interfaces within the wireless communications system for the purpose of
5 intercepting messages important to the Wireless Location System for identifying wireless transmitters and the RF channels in use by these transmitters. These interfaces may include, for example, the "A interface" and "Abis interface" used in wireless communications systems employing the GSM air interface protocol. (This aspect of the present invention is described in greater detail below in the section titled "Monitoring of
10 Call Information".) These interfaces are well known and published in various standards. By monitoring the bi-directional messages on these interfaces between base stations (BTS), base station controllers (BSC), and mobile switching centers (MSC), and other points, the Wireless Location System can obtain the same information about the assignment of wireless transmitters to specific channels as the wireless communications
15 system itself knows. The Wireless Location System includes means to monitor these interfaces at various points. For example, the SCS 10 may monitor a BTS to BSC interface. Alternately, a TLP 12 or AP 14 may also monitor a BSC where a number of BTS to BSC interfaces have been concentrated. The interfaces internal to the wireless communications system are not encrypted and the layered protocols are known to those
20 familiar with the art. The advantage to the Wireless Location System to monitoring these interfaces is that the Wireless Location System may not be required to independently detect and demodulate control channel messages from wireless transmitters. In addition, the Wireless Location System may obtain all necessary voice channel assignment information from these interfaces.

25

Using these means for a control channel transmission, the SCS 10 receives the transmissions as described earlier and records the control channel RF data into memory without performing detection and demodulation. Separately, the Wireless Location System monitors the messages occurring over prescribed interfaces within the wireless
30 communications system, and causes a trigger in the Wireless Location System when the Wireless Location System discovers a message containing a trigger event. Initiated by the trigger event, the Wireless Location System determines the approximately time at

which the wireless transmission occurred, and commands a first SCS 10 and a second SCS 10B to each search its memory for the start of transmission. This first SCS 10A chosen is an SCS that is either collocated with the base station to which the wireless transmitter had communicated, or an SCS which is adjacent to the base station to which the wireless transmitter had communicated. That is, the first SCS 10A is an SCS which would have been assigned the control channel as a primary channel. If the first SCS 10A successfully determines and reports the start of the transmission, then location processing proceeds normally, using the means described below. If the first SCS 10A cannot successfully determine the start of transmission, then the second SCS 10B reports the start of transmission, and then location processing proceeds normally.

The Wireless Location System also uses these means for voice channel transmissions. For all triggers contained in the Tasking List, the Wireless Location System monitors the prescribed interfaces for messages pertaining to those triggers. The messages of interest include, for example, voice channel assignment messages, handoff messages, frequency hopping messages, power up / power down messages, directed re-try messages, termination messages, and other similar action and status messages. The Wireless Location System continuously maintains a copy of the state and status of these wireless transmitters in a State Table in the AP 14. Each time that the Wireless Location System detects a message pertaining to one of the entries in the Tasking List, the Wireless Location System updates its own State Table. Thereafter, the Wireless Location System may trigger to perform location processing, such as on a regular time interval, and access the State Table to determine precisely which cell site, sector, RF channel, and timeslot is presently being used by the wireless transmitter. The example contained herein described the means by which the Wireless Location System interfaces to a GSM based wireless communications system. The Wireless Location System also supports similar functions with systems based upon other air interfaces.

For certain air interfaces, such as CDMA, the Wireless Location System also keeps certain identity information obtained from Access bursts in the control channel in the State Table; this information is later used for decoding the masks used for voice channels. For example, the CDMA air interface protocol uses the Electronic Serial

Number (ESN) of a wireless transmitter to, in part, determine the long code mask used in the coding of voice channel transmissions. The Wireless Location System maintains this information in the State Table for entries in the Tasking List because many wireless transmitters may transmit the information only once; for example, many CDMA mobiles will only transmit their ESN during the first Access burst after the wireless transmitter become active in a geographic area. This ability to independently determine the long code mask is very useful in cases where an interface between the Wireless Location System and the wireless communications system is not operative and/or the Wireless Location System is not able to monitor one of the interfaces internal to the wireless communications system. The operator of the Wireless Location System may optionally set the Wireless Location System to maintain the identity information for all wireless transmitters. In addition to the above reasons, the Wireless Location System can provide the voice channel tracking for all wireless transmitters that trigger location processing by calling "911". As described earlier, the Wireless Location System uses dynamic tasking to provide location to a wireless transmitter for a prescribed time after dialing "911", for example. By maintaining the identity information for all wireless transmitters in the State Table, the Wireless Location System is able to provide voice channel tracking for all transmitters in the event of a prescribed trigger event, and not just those with prior entries in the Tasking List.

20

Applications Interface

Using the AP 14, the Wireless Location System supports a variety of standards based interfaces to end-user and carrier location applications using secure protocols such as TCP/IP, X.25, SS-7, and IS-41. Each interface between the AP 14 and an external application is a secure and authenticated connection that permits the AP 14 to positively verify the identity of the application that is connected to the AP 14. This is necessary because each connected application is granted only limited access to location records on a real-time and/or historical basis. In addition, the AP 14 supports additional command / response, real-time, and post-processing functions that are further detailed below. Access to these additional functions also requires authentication. The AP 14 maintains a user list and the authentication means associated with each user. No application can gain access to location records or functions for which the application does not have proper

authentication or access rights. In addition, the AP 14 supports full logging of all actions taken by each application in the event that problems arise or a later investigation into actions is required. For each command or function in the list below, the AP 14 preferably supports a protocol in which each action or the result of each is confirmed, as
5 appropriate.

Edit Tasking List – This command permits external applications to add, remove, or edit entries in the Tasking List, including any fields and flags associated with each entry. This command can be supported on a single entry basis, or a batch entry basis where a
10 list of entries is included in a single command. The latter is useful, for example, in a bulk application such as location sensitive billing whereby larger volumes of wireless transmitters are being supported by the external application, and it is desired to minimize protocol overhead. This command can add or delete applications for a particular entry in the Tasking List, however, this command cannot delete an entry entirely if the entry also
15 contains other applications not associated with or authorized by the application issuing the command.

Set Location Interval – The Wireless Location System can be set to perform location processing at any interval for a particular wireless transmitter, on either control or voice
20 channels. For example, certain applications may require the location of a wireless transmitter every few seconds when the transmitter is engaged on a voice channel. When the wireless transmitter make an initial transmission, the Wireless Location System initially triggers using a standard entry in the Tasking List. If one of the fields or flags in this entry specifies updated location on a set interval, then the Wireless Location System
25 creates a dynamic task in the Tasking List that is triggered by a timer instead of an identity or other transmitted criteria. Each time the timer expires, which can range from 1 second to several hours, the Wireless Location System will automatically trigger to locate the wireless transmitter. The Wireless Location System uses its interface to the wireless communications system to query status of the wireless transmitter, including
30 voice call parameters as described earlier. If the wireless transmitter is engaged on a voice channel, then the Wireless Location System performs location processing. If the wireless transmitter is not engaged in any existing transmissions, the Wireless Location

System will command the wireless communications system to make the wireless transmitter immediately transmit. When the dynamic task is set, the Wireless Location System also sets an expiration time at which the dynamic task ceases.

- 5 End-User Addition / Deletion – This command can be executed by an end-user of a wireless transmitter to place the identity of the wireless transmitter onto the Tasking List with location processing enabled, to remove the identity of the wireless transmitter from the Tasking List and therefore eliminate identity as a trigger, or to place the identity of the wireless transmitter onto the Tasking List with location processing disabled. When
- 10 location processing has been disabled by the end-user, known as Prohibit Location Processing then no location processing will be performed for the wireless transmitter. The operator of the Wireless Location System can optionally select one of several actions by the Wireless Location System in response to a Prohibit Location Processing command by the end user: (i) the disabling action can override all other triggers in the
- 15 Tasking List, including a trigger due to an emergency call such as “911”, (ii) the disabling action can override any other trigger in the Tasking List, except a trigger due to an emergency call such as “911”, (iii) the disabling action can be overridden by other select triggers in the Tasking List. In the first case, the end-user is granted complete control over the privacy of the transmissions by the wireless transmitter, as no location
- 20 processing will be performed on that transmitter for any reason. In the second case, the end-user may still receive the benefits of location during an emergency, but at no other times. In an example of the third case, an employer who is the real owner of a particular wireless transmitter can override an end-user action by an employee who is using the wireless transmitter as part of the job but who may not desire to be located. The Wireless
- 25 Location System may query the wireless communications system, as described above, to obtain the mapping of the identity contained in the wireless transmission to other identities.

- The additions and deletions by the end-user are effected by dialed sequences of
- 30 characters and digits and pressing the “SEND” or equivalent button on the wireless transmitter. These sequences may be optionally chosen and made known by the operator of the Wireless Location System. For example, one sequence may be “*55 SEND” to

disable location processing. Other sequences are also possible. When the end-user can dialed this prescribed sequence, the wireless transmitter will transmit the sequence over one of the prescribed control channels of the wireless communications system. Since the Wireless Location System independently detects and demodulates all reverse control

5 channel transmissions, the Wireless Location System can independently interpret the prescribed dialed sequence and make the appropriate feature updates to the Tasking List, as described above. When the Wireless Location System has completed the update to the Tasking List, the Wireless Location System commands the wireless communications system to send a confirmation to the end-user. As described earlier, this may take the

10 form of an audible tone, recorded or synthesized voice, or a text message. This command is executed over the interface between the Wireless Location System and the wireless communications system.

Command Transmit – This command allows external applications to cause the Wireless

15 Location System to send a command to the wireless communications system to make a particular wireless transmitter, or group of wireless transmitters, transmit. This command may contain a flag or field that the wireless transmitter(s) should transmit immediately or at a prescribed time. This command has the effort of locating the wireless transmitter(s) upon command, since the transmissions will be detected, demodulated, and triggered,

20 causing location processing and the generation of a location record. This is useful in eliminating or reducing any delay in determining location such as waiting for the next registration time period for the wireless transmitter or waiting for an independent transmission to occur.

25 External Database Query and Update – The Wireless Location System includes means to access an external database, to query the said external database using the identity of the wireless transmitter or other parameters contained in the transmission or the trigger criteria, and to merge the data obtained from the external database with the data generated by the Wireless Location System to create a new enhanced location record.

30 The enhanced location record may then be forwarded to requesting applications. The external database may contain, for example, data elements such as customer information, medical information, subscribed features, application related information, customer

account information, contact information, or sets of prescribed actions to take upon a location trigger event. The Wireless Location System may also cause updates to the external database, for example, to increment or decrement a billing counter associated with the provision of location services, or to update the external database with the latest
5 location record associated with the particular wireless transmitter. The Wireless Location System contains means to performed the actions described herein on more than one external database. The list and sequence of external databases to access and the subsequent actions to take are contained in one of the fields contained in the trigger criteria in the Tasking List.

10

Random Anonymous Location Processing – The Wireless Location System includes means to perform large scale random anonymous location processing. This function is valuable to certain types of applications that require the gathering of a large volume of data about a population of wireless transmitters without consideration to the specific
15 identities of the individual transmitters. Applications of this type include: RF Optimization, which enables wireless carriers to measure the performance of the wireless communications system by simultaneously determining location and other parameters of a transmission; Traffic Management, which enables government agencies and commercial concerns to monitor the flow of traffic on various highways using
20 statistically significant samples of wireless transmitters travelling in vehicles; and Local Traffic Estimation, which enables commercial enterprises to estimate the flow of traffic around a particular area which may help determine the viability of particular businesses.

Applications requesting random anonymous location processing optionally receive
25 location records from two sources: (i) a copy of location records generated for other applications, and (ii) location records which have been triggered randomly by the Wireless Location System without regard to any specific criteria. All of the location records generated from either source are forwarded with all of the identity and trigger criteria information removed from the location records; however, the requesting
30 application(s) can determine whether the record was generated from the fully random process or is a copy from another trigger criteria. The random location records are generated by a low priority task within the Wireless Location System that performs

location processing on randomly selected transmissions whenever processing and communications resources are available and would otherwise be unused at a particular instant in time. The requesting application(s) can specify whether the random location processing is performed over the entire coverage area of a Wireless Location System, 5 over specific geographic areas such as along prescribed highways, or by the coverage areas of specific cell sites. Thus, the requesting application(s) can direct the resources of the Wireless Location System to those area of greatest interest to each application. Depending on the randomness desired by the application(s), the Wireless Location System can adjust preferences for randomly selecting certain types of transmissions, for 10 example, registration messages, origination messages, page response messages, or voice channel transmissions.

Anonymous Tracking of a Geographic Group – The Wireless Location System includes means to trigger location processing on a repetitive basis for anonymous groups of 15 wireless transmitters within a prescribed geographic area. For example, a particular location application may desire to monitor the travel route of a wireless transmitter over a prescribed period of time, but without the Wireless Location System disclosing the particular identity of the wireless transmitter. The period of time may be many hours, days, or weeks. Using the means, the Wireless Location System: randomly selects a 20 wireless transmitter that initiates a transmission in the geographic area of interest to the application; performs location processing on the transmission of interest; irreversibly translates and encrypts the identity of the wireless transmitter into a new coded identifier; creates a location record using only the new coded identifier as an identifying means; forwards the location record to the requesting location application(s); and creates a 25 dynamic task in the Tasking List for the wireless transmitter, wherein the dynamic task has an associated expiration time. Subsequently, whenever the prescribed wireless transmitter initiates transmission, the Wireless Location System may trigger using the dynamic task, perform location processing on the transmission of interest, irreversibly translate and encrypt the identity of the wireless transmitter into the new coded identifier 30 using the same means as prior such that the coded identifier is the same, create a location record using the coded identifier, and forward the location record to the requesting location application(s). The means described herein can be combined with other

functions of the Wireless Location System to perform this type of monitoring use either control or voice channel transmissions. Further, the means described herein completely preserve the private identity of the wireless transmitter, yet enables another class of applications that can monitor the travel patterns of wireless transmitters. This class of applications can be of great value in determining the planning and design of new roads, alternate route planning, or the construction of commercial and retail space.

Location Record Grouping, Sorting, and Labeling – The Wireless Location System include means to post-process the location records for certain requesting applications to group, sort, or label the location records. For each interface supported by the Wireless Location System, the Wireless Location System stores a profile of the types of data for which the application is both authorized and requesting, and the types of filters or post-processing actions desired by the application. Many applications, such as the examples contained herein, do not require individual location records or the specific identities of individual transmitters. For example, an RF optimization application derives more value from a large data set of location records for a particular cell site or channel than it can from any individual location record. For another example, a traffic monitoring application requires only location records from transmitters that are on prescribed roads or highways, and additionally requires that these records be grouped by section of road or highway and by direction of travel. Other applications may request that the Wireless Location System forward location records that have been formatted to enhance visual display appeal by, for example, adjusting the location estimate of the transmitter so that the transmitter's location appears on an electronic map directly on a drawn road segment rather than adjacent to the road segment. Therefore, the Wireless Location System preferably "snaps" the location estimate to the nearest drawn road segment.

The Wireless Location System can filter and report location records to an application for wireless transmitters communicating only on a particular cell site, sector, RF channel, or group of RF channels. Before forwarding the record to the requesting application, the Wireless Location System first verifies that the appropriate fields in the record satisfy the requirements. Records not matching the requirements are not forwarded, and records matching the requirements are forwarded. Some filters are geographic and must be

calculated by the Wireless Location System. For example, the Wireless Location System can process a location record to determine the closest road segment and direction of travel of the wireless transmitter on the road segment. The Wireless Location System can then forward only records to the application that are determined to be on a particular road segment, and can further enhance the location record by adding a field containing the determined road segment. In order to determine the closest road segment, the Wireless Location System is provided with a database of road segments of interest by the requesting application. This database is stored in a table where each road segment is stored with a latitude and longitude coordinate defining the end point of each segment.

Each road segment can be modeled as a straight or curved line, and can be modeled to support one or two directions of travel. Then for each location record determined by the Wireless Location System, the Wireless Location System compares the latitude and longitude in the location record to each road segment stored in the database, and determines the shortest distance from a modeled line connecting the end points of the segment to the latitude and longitude of the location record. The shortest distance is a calculated imaginary line orthogonal to the line connecting the two end points of the stored road segment. When the closest road segment has been determined, the Wireless Location System can further determine the direction of travel on the road segment by comparing the direction of travel of the wireless transmitter reported by the location processing to the orientation of the road segment. The direction that produces the smallest error with respect to the orientation of the road segments is then reported by the Wireless Location System.

Network Operations Console (NOC) 16

The NOC 16 is a network management system that permits operators of the Wireless Location System easy access to the programming parameters of the Wireless Location System. For example, in some cities, the Wireless Location System may contain many hundreds or even thousands of SCS's 10. The NOC is the most effective way to manage a large Wireless Location System, using graphical user interface capabilities. The NOC will also receive real time alerts if certain functions within the Wireless Location System are not operating properly. These real time alerts can be used by the operator to take corrective action quickly and prevent a degradation of location

service. Experience with trials of the Wireless Location System show that the ability of the system to maintain good location accuracy over time is directly related to the operator's ability to keep the system operating within its predetermined parameters.

5 Location Processing

The Wireless Location System is capable of performing location processing using two different methods known as central based processing and station based processing. Both techniques were first disclosed in Patent Number 5,327,144, and are further enhanced in this specification. Location processing depends in part on the ability to accurately determine certain phase characteristics of the signal as received at multiple antennas and at multiple SCS's 10. Therefore, it is an object of the Wireless Location System to identify and remove sources of phase error that impede the ability of the location processing to determine the phase characteristics of the received signal. One source of phase error is inside of the wireless transmitter itself, namely the oscillator (typically a crystal oscillator) and the phase lock loops that allow the phone to tune to specific channels for transmitting. Lower cost crystal oscillators will generally have higher phase noise. Some air interface specifications, such as IS-136 and IS-95A, have specifications covering the phase noise with which a wireless telephone can transmit. Other air interface specifications, such as IS-553A, do not closely specify phase noise. It is therefore an object of the present invention to automatically reduce and/or eliminate a wireless transmitter's phase noise as a source of phase error in location processing, in part by automatically selecting the use of central based processing or station based processing. The automatic selection will also consider the efficiency with which the communications link between the SCS 10 and the TLP 12 is used, and the availability of DSP resources at each of the SCS 10 and TLP 12.

When using central based processing, the TDOA and FDOA determination and the multipath processing are performed in the TLP 12 along with the position and speed determination. This method is preferred when the wireless transmitter has a phase noise that is above a predetermined threshold. In these cases, central based processing is most effective in reducing or eliminating the phase noise of the wireless transmitter as a source of phase error because the TDOA estimate is performed using a digital

representation of the actual RF transmission from two antennas, which may be at the same SCS 10 or different SCS's 10. In this method, those skilled in the art will recognize that the phase noise of the transmitter is a common mode noise in the TDOA processing, and therefore is self-canceling in the TDOA determination process. This method works
5 best, for example, with many very low cost AMPS cellular telephones that have a high phase noise. The basic steps in central based processing include the steps recited below and represented in the flowchart of Figure 6:

a wireless transmitter initiates a transmission on either a control channel or a voice
10 channel (step S50);
the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S51);
the transmission is converted into a digital format in the receiver connected to each SCS/antenna (step S52);
15 the digital data is stored in a memory in the receivers in each SCS 10 (step S53);
the transmission is demodulated (step S54);
the Wireless Location System determines whether to begin location processing for the transmission (step S55);
if triggered, the TLP 12 requests copies of the digital data from the memory in
20 receivers at multiple SCS's 10 (step S56);
digital data is sent from multiple SCS's 10 to a selected TLP 12 (step S57);
the TLP 12 performs TDOA, FDOA, and multipath mitigation on the digital data from pairs of antennas (step S58);
the TLP 12 performs position and speed determination using the TDOA data, and then
25 creates a location record and forwards the location record to the AP 14 (step S59).

The Wireless Location System uses a variable number of bits to represent the transmission when sending digital data from the SCS's 10 to the TLP 12. As discussed earlier, the SCS receiver digitizes wireless transmissions with a high resolution, or a high
30 number of bits per digital sample in order to achieve a sufficient dynamic range. This is especially required when using wideband digital receivers, which may be simultaneously receiving signals near to the SCS 10A and far from the SCS 10B. For example, up to 14

bits may be required to represent a dynamic range of 84 dB. Location processing does not always require the high resolution per digital sample, however. Frequently, locations of sufficient accuracy are achievable by the Wireless Location System using a fewer number of bits per digital sample. Therefore, to minimize the implementation cost of the

5 Wireless Location System by conserving bandwidth on the communication links between each SCS 10 and TLP 12, the Wireless Location System determines the fewest number of bits required to digitally represent a transmission while still maintaining a desired accuracy level. This determination is based, for example, on the particular air interface protocol used by the wireless transmitter, the SNR of the transmission, the

10 degree to which the transmission has been perturbed by fading and/or multipath, and the current state of the processing and communication queues in each SCS 10. The number of bits sent from the SCS 10 to the TLP 12 are reduced in two ways: the number of bits per sample is minimized, and the shortest length, or fewest segments, of the transmission possible is used for location processing. The TLP 12 can use this minimal RF data to

15 perform location processing and then compare the result with the desired accuracy level. This comparison is performed on the basis of a confidence interval calculation. If the location estimate does not fall within the desired accuracy limits, the TLP 12 will recursively request additional data from selected SCS's 10. The additional data may include an additional number of bits per digital sample and/or may include more

20 segments of the transmission. This process of requesting additional data may continue recursively until the TLP 12 has achieved the prescribed location accuracy.

There are additional details to the basic steps described above. These details are described in prior Patent Numbers 5,327,144 and 5,608,410 in other parts of this

25 specification. One enhancement to the processes described in earlier patents is the selection of a single reference SCS/antenna that is used for each baseline in the location processing. In prior art, baselines were determined using pairs of antenna sites around a ring. In the present Wireless Location System, the single reference SCS/antenna used is generally the highest SNR signal, although other criteria are also used as described

30 below. The use of a high SNR reference aids central based location processing when the other SCS/antennas used in the location processing are very weak, such as at or below the noise floor (i.e. zero or negative signal to noise ratio). When station based location

processing is used, the reference signal is a re-modulated signal, which is intentionally created to have a very high signal to noise ratio, further aiding location processing for very weak signals at other SCS/antennas. The actual selection of the reference SCS/antenna is described below.

5

The Wireless Location System mitigates multipath by first recursively estimating the components of multipath received in addition to the direct path component and then subtracting these components from the received signal. Thus the Wireless Location System models the received signal and compares the model to the actual received signal
10 and attempts to minimize the difference between the two using a weighted least square difference. For each transmitted signal $x(t)$ from a wireless transmitter, the received signal $y(t)$ at each SCS/antenna is a complex combination of signals:

$$y(t) = \sum x(t - \tau_n) a_n e^{j\omega(t - \tau_n)}, \text{ for all } n = 0 \text{ to } N;$$

15

where $x(t)$ is the signal as transmitted by the wireless transmitter;
 a_n and τ_n are the complex amplitude and delays of the multipath components;
 N is the total number of multipath components in the received signal; and
 a_0 and τ_0 are constants for the most direct path component.

20

The operator of the Wireless Location System empirically determines a set of constraints for each component of multipath that applies to the specific environment in which each Wireless Location System is operating. The purpose of the constraints is to limit the amount of processing time that the Wireless Location System spends optimizing the
25 results for each multipath mitigation calculation. For example, the Wireless Location System may be set to determine only four components of multipath: the first component may be assumed to have a time delay in the range τ_{1A} to τ_{1B} ; the second component may be assumed to have a time delay in the range τ_{2A} to τ_{2B} ; the third component may be assumed to have a time delay in the range τ_{3A} to τ_{3B} ; and similar for the fourth
30 component; however the fourth component is a single value that effectively represents a complex combination of many tens of individual (and somewhat diffuse) multipath

components whose time delays exceed the range of the third component. For ease of processing, the Wireless Location System transforms the prior equation into the frequency domain, and then solves for the individual components such that a weighted least squares difference is minimized.

5

When using station based processing, the TDOA and FDOA determination and multipath mitigation are performed in the SCS's 10, while the position and speed determination are typically performed in the TLP 12. The main advantage of station based processing, as described in Patent Number 5,327,144, is reducing the amount of data that is sent on the communication link between each SCS 10 and TLP 12. However, there may be other advantages as well. One new objective of the present invention is increasing the effective signal processing gain during the TDOA processing. As pointed out earlier, central based processing has the advantage of eliminating or reducing phase error caused by the phase noise in the wireless transmitter. However, no previous disclosure has addressed how to eliminate or reduce the same phase noise error when using station based processing. The present invention reduces the phase error and increases the effective signal processing gain using the steps recited below and shown in Figure 6:

a wireless transmitter initiates a transmission on either a control channel or a voice channel (step S60);
the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S61);
the transmission is converted into a digital format in the receiver connected to each antenna (step S62);
the digital data is stored in a memory in the SCS 10 (step S63);
the transmission is demodulated (step S64);
the Wireless Location System determines whether to begin location processing for the transmission (step S65);
if triggered, a first SCS 10A demodulates the transmission and determines an appropriate phase correction interval (step S66);
for each such phase correction interval, the first SCS 10A calculates an appropriate phase correction and amplitude correction, and encodes this phase correction

- parameter and amplitude correction parameter along with the demodulated data (step S67);
- the demodulated data and phase correction and amplitude correction parameters are sent from the first SCS 10A to a TLP 12 (step S68);
- 5 the TLP 12 determines the SCS's 10 and receiving antennas to use in the location processing (step S69);
- the TLP 12 sends the demodulated data and phase correction and amplitude correction parameters to each second SCS 10B that will be used in the location processing (step S70);
- 10 the first SCS 10 and each second SCS 10B creates a first re-modulated signal based upon the demodulated data and the phase correction and amplitude correction parameters (step S71);
- the first SCS 10A and each second SCS 10B performs TDOA, FDOA, and multipath mitigation using the digital data stored in memory in each SCS 10 and the first re-
- 15 modulated signal (step S72);
- the TDOA, FDOA, and multipath mitigation data are sent from the first SCS 10A and each second SCS 10B to the TLP 12 (step S73);
- the TLP 12 performs position and speed determination using the TDOA data (step S74); and
- 20 the TLP 12 creates a location record, and forwards the location record to the AP 14 (step S75).

The advantages of determining phase correction and amplitude correction parameters are most obvious in the location of CDMA wireless transmitters based upon IS-95A. As is

25 well known, the reverse transmissions from an IS-95A transmitter are sent using non-coherent modulation. Most CDMA base stations only integrate over a single bit interval because of the non-coherent modulation. For a CDMA Access Channel, with a bit rate of 4800 bits per second, there are 256 chips sent per bit, which permits an integration gain of 24 dB. Using the technique described above, the TDOA processing in each SCS 10

30 may integrate, for example, over a full 160 millisecond burst (196,608 chips) to produce an integration gain of 53 dB. This additional processing gain enables the present

invention to detect and locate CDMA transmissions using multiple SCS's 10, even if the base stations collocated with the SCS's 10 cannot detect the same CDMA transmission.

For a particular transmission, if either the phase correction parameters or the amplitude
5 correction parameters are calculated to be zero, or are not needed, then these parameters are not sent in order to conserve on the number of bits transmitted on the communications link between each SCS 10 and TLP 12. In another embodiment of the invention, the Wireless Location System may use a fixed phase correction interval for a particular transmission or for all transmissions of a particular air interface protocol, or
10 for all transmissions made by a particular type of wireless transmitter. This may, for example, be based upon empirical data gathered over some period of time by the Wireless Location System showing a reasonable consistency in the phase noise exhibited by various classes of transmitters. In these cases, the SCS 10 may save the processing step of determining the appropriate phase correction interval.

15 Those skilled in the art will recognize that there are many ways of measuring the phase noise of a wireless transmitter. In one embodiment, a pure, noiseless re-modulated copy of the signal received at the first SCS 10A may be digitally generated by DSP's in the SCS, then the received signal may be compared against the pure signal over each phase
20 correction interval and the phase difference may be measured directly. In this embodiment, the phase correction parameter will be calculated as the negative of the phase difference over that phase correction interval. The number of bits required to represent the phase correction parameter will vary with the magnitude of the phase correction parameter, and the number of bits may vary for each phase correction interval.
25 It has been observed that some transmissions, for example, exhibit greater phase noise early in the transmission, and less phase noise in the middle of and later in the transmission.

Station based processing is most useful for wireless transmitters that have relatively low
30 phase noise. Although not necessarily required by their respective air interface standards, wireless telephones that use the TDMA, CDMA, or GSM protocols will typically exhibit lower phase noise. As the phase noise of a wireless transmitter increases, the length of a

phase correction interval may decrease and/or the number of bits required to represent the phase correction parameters increases. Station based processing is not effective when the number of bits required to represent the demodulated data plus the phase correction and amplitude parameters exceeds a predetermined proportion of the number of bits
5 required to perform central based processing. It is therefore an object of the present invention to automatically determine for each transmission for which a location is desired whether to process the location using central based processing or station based processing. The steps in making this determination are recited below and shown in Figure 7:

10 a wireless transmitter initiates a transmission on either a control channel or a voice channel (step S80);
the transmission is received at a first SCS 10A (step S81);
the transmission is converted into a digital format in the receiver connected to each
15 antenna (step S82);
the Wireless Location System determines whether to begin location processing for the transmission (step S83);
if triggered, a first SCS 10A demodulates the transmission and estimates an appropriate phase correction interval and the number of bits required to encode the phase
20 correction and amplitude correction parameters (step S84);
the first SCS 10A then estimates the number of bits required for central based processing;
based upon the number of bits required for each respective method, the SCS 10 or the TLP 12 determine whether to use central based processing or station based
25 processing to perform the location processing for this transmission (step S85).

In another embodiment of the invention, the Wireless Location System may always use central based processing or station based processing for all transmissions of a particular air interface protocol, or for all transmissions made by a particular kind of wireless
30 transmitter. This may, for example, be based upon empirical data gathered over some period of time by the Wireless Location System showing a reasonable consistency in the phase noise exhibited by various classes of transmitters. In these cases, the SCS 10

and/or the TLP 12 may be saved the processing step of determining the appropriate processing method.

A further enhancement of the present invention, used for both central based processing and station based processing, is the use of threshold criteria for including baselines in the final determination of location and velocity of the wireless transmitter. For each baseline, the Wireless Location System calculates a number of parameters that include: the SCS/antenna port used with the reference SCS/antenna in calculating the baseline, the peak, average, and variance in the power of the transmission as received at the SCS/antenna port used in the baseline and over the interval used for location processing, the correlation value from the cross-spectra correlation between the SCS/antenna used in the baseline and the reference SCS/antenna, the delay value for the baseline, the multipath mitigation parameters, the residual values remaining after the multipath mitigation calculations, the contribution of the SCS/antenna to the weighted GDOP in the final location solution, and a measure of the quality of fit of the baseline if included in the final location solution. Each baseline is included in the final location solution is each meets or exceeds the threshold criteria for each of the parameters described herein. A baseline may be excluded from the location solution if it fails to meet one or more of the threshold criteria. Therefore, it is frequently possible that the number of SCS/antennas actually used in the final location solution is less than the total number considered.

Previous Patent Numbers 5,327,144 and 5,608,410 disclosed a method by which the location processing minimized the least square difference (LSD) value of the following equation:

$$\text{LSD} = [Q_{12}(\text{Delay_T}_{12} - \text{Delay_O}_{12})^2 + Q_{13}(\text{Delay_T}_{13} - \text{Delay_O}_{13})^2 + \dots + Q_{xy}(\text{Delay_T}_{xy} - \text{Delay_O}_{xy})^2]$$

In the present implementation, this equation has been rearranged to the following form in order to make the location processing code more efficient:

$$\text{LSD} = \sum (\text{TDOA}_{0i} - \tau_i + \tau_0)^2 w_i^2; \text{ over all } i=1 \text{ to } N-1$$

where N = number of SCS/antennas used in the location processing;

TDOA_{0i} = the TDOA to the i^{th} site from reference site 0;

5 τ_i = the theoretical line of sight propagation time from the wireless transmitter to the i^{th} site;

τ_0 = the theoretical line of sight propagation time from the transmitter to the reference;
and

w_i = the weight, or quality factor, applied to the i^{th} baseline.

10

In the present implementation, the Wireless Location System also uses another alternate form of the equation that can aid in determining location solutions when the reference signal is not very strong or when it is likely that a bias would exist in the location solution using the prior form of the equation:

15

$$\text{LSD}' = \sum (\text{TDOA}_{0i} - \tau_i)^2 w_i^2 - b^2 \sum w_i^2; \text{ over all } i=0 \text{ to } N-1$$

Where N = number of SCS/antennas used in the location processing;

TDOA_{0i} = the TDOA to the i^{th} site from reference site 0;

20 TDOA_{00} = is assumed to be zero;

τ_i = the theoretical line of sight propagation time from the wireless transmitter to the i^{th} site;

b = a bias that is separately calculated for each theoretical point that minimizes LSD' at that theoretical point; and

25 w_i = the weight, or quality factor, applied to the i^{th} baseline.

The LSD' form of the equation offers an easier means of removing a bias in location solutions at the reference site by making w_0 equal to the maximum value of the other weights or basing w_0 on the relative signal strength at the reference site. Note that if w_0 is
30 much larger than the other weights, then b is approximately equal to τ_0 . In general, the weights, or quality factors are based on similar criteria to that discussed above for the

threshold criteria in including baselines. That is, the results of the criteria calculations are used for weights and when the criteria falls below threshold the weight is then set to zero and is effectively not included in the determination of the final location solution.

5 Antenna Selection Process for Location Processing

Previous inventions and disclosures, such as those listed above, have described techniques in which a first, second, or possibly third antenna site, cell site, or base station are required to determine location. Patent number 5,608,410 further discloses a Dynamic Selection Subsystem (DSS) that is responsible for determining which data frames from
10 which antenna site locations will be used to calculate the location of a responsive transmitter. In the DSS, if data frames are received from more than a threshold number of sites, the DSS determines which are candidates for retention or exclusion, and then dynamically organizes data frames for location processing. The DSS prefers to use more than the minimum number of antenna sites so that the solution is over-determined.
15 Additionally, the DSS assures that all transmissions used in the location processing were received from the same transmitter and from the same transmission.

The preferred embodiments of the prior inventions had several limitations, however. First, either only one antenna per antenna site (or cell site) is used, or the data from two
20 or four diversity antennas were first combined at the antenna site (or cell site) prior to transmission to the central site. Additionally, all antenna sites that received the transmission sent data frames to the central site, even if the DSS later discarded the data frames. Thus, some communications bandwidth may have been wasted sending data that was not used.

25

The present inventors have determined that while a minimum of two or three sites are required in order determine location, the actual selection of antennas and SCS's 10 to use in location processing can have a significant effect on the results of the location processing. In addition, it is advantageous to include the means to use more than one
30 antenna at each SCS 10 in the location processing. The reason for using data from multiple antennas at a cell site independently in the location processing is that the signal received at each antenna is uniquely affected by multipath, fading, and other

disturbances. It is well known in the field that when two antennas are separated in distance by more than one wavelength, then each antenna will receive the signal on an independent path. Therefore, there is frequently additional and unique information to be gained about the location of the wireless transmitter by using multiple antennas, and the
5 ability of the Wireless Location System to mitigate multipath is enhanced accordingly.

It is therefore an object of the present invention to provide an improved method for using the signals received from more than one antenna at an SCS 10 in the location processing. It is a further object to provide a method to improve the dynamic process used to select
10 the cooperating antennas and SCS's 10 used in the location processing. The first object is achieved by providing means within the SCS 10 to select and use any segment of data collected from any number of antennas at an SCS in the location processing. As described earlier, each antenna at a cell site is connected to a receiver internal to the SCS 10. Each receiver converts signals received from the antenna into a digital form, and then
15 stores the digitized signals temporarily in a memory in the receiver. The TLP 12 has been provided with means to direct any SCS 10 to retrieve segments of data from the temporary memory of any receiver, and to provide the data for use in location processing. The second object is achieved by providing means within the Wireless Location System to monitor a large number of antennas for reception of the transmission
20 that the Wireless Location System desires to locate, and then selecting a smaller set of antennas for use in location processing based upon a predetermined set of parameters.

One example of this selection process is represented by the flowchart of Figure 8:
a wireless transmitter initiates a transmission on either a control channel or a voice
25 channel (step S90);
the transmission is received at multiple antennas and at multiple SCS's 10 in the Wireless Location System (step S91);
the transmission is converted into a digital format in the receiver connected to each antenna (step S92);
30 the digital data is stored in a memory in each SCS 10 (step S93);

- the transmission is demodulated at at least one SCS 10A and the channel number on which the transmission occurred and the cell site and sector serving the wireless transmitter is determined (step S94);
- based upon the serving cell site and sector, one SCS 10A is designated as the 'primary' SCS 10 for processing that transmission (step S95);
- the primary SCS 10A determines a timestamp associated with the demodulated data (step S96);
- the Wireless Location System determines whether to begin location processing for the transmission (step S97);
- if location processing is triggered, the Wireless Location System determines a candidate list of SCS's 10 and antennas to use in the location processing (step S98);
- each candidate SCS/antenna measures and reports several parameters in the channel number of the transmission and at the time of the timestamp determined by the primary SCS 10A (step S99);
- the Wireless Location System orders the candidate SCS/antennas using specified criteria and selects a reference SCS/antenna and a processing list of SCS/antennas to use in the location processing (step S100); and
- the Wireless Location System proceeds with location processing as described earlier, using data from the processing list of SCS/antennas (step S101).

20

Selecting Primary SCS/Antenna

- The process for choosing the 'primary' SCS/antenna is critical, because the candidate list of SCS's 10 and antennas 10-1 is determined in part based upon the designation of the primary SCS/antenna. When a wireless transmitter makes a transmission on a particular RF channel, the transmission frequently can propagate many miles before the signal attenuates below a level at which it can be demodulated. Therefore, there are frequently many SCS/antennas capable of demodulating the signal. This especially occurs in urban and suburban areas where the frequency re-use pattern of many wireless communications systems can be quite dense. For example, because of the high usage rate of wireless and the dense cell site spacing, the present inventors have tested wireless communications systems in which the same RF control channel and digital color code were used on cell sites spaced about one mile apart. Because the

- Wireless Location System is independently demodulating these transmissions, the Wireless Location System frequently can demodulate the same transmission at two, three, or more separate SCS/antennas. The Wireless Location System detects that the same transmission has been demodulated multiple times at multiple SCS/antennas when
- 5 the Wireless Location System receives multiple demodulated data frames sent from different SCS/antennas, each with a number of bit errors below a predetermined bit error threshold, and with the demodulated data matching within an acceptable limit of bit errors, and all occurring within a predetermined interval of time.
- 10 When the Wireless Location System detects demodulated data from multiple SCS/antennas, it examines the following parameters to determine which SCS/antenna may be designated the primary SCS: average SNR over the transmission interval used for location processing, the variance in the SNR over the same interval, correlation of the beginning of the received transmission against a pure pre-cursor (i.e. for AMPS, the
- 15 dotting and Barker code), the number of bit errors in the demodulated data, and the magnitude and rate of change of the SNR from just before the on-set of the transmission to the on-set of the transmission, as well as other similar parameters. The average SNR is typically determined at each SCS/antenna either over the entire length of the transmission to be used for location processing, or over a shorter interval. The average
- 20 SNR over the shorter interval can be determined by performing a correlation with the dotting sequence and/or Barker code and/or sync word, depending on the particular air interface protocol, and over a short range of time before, during, and after the timestamp reported by each SCS 10. The time range may typically be +/-200 microseconds centered at the timestamp, for example. The Wireless Location System will generally order the
- 25 SCS/antennas using the following criteria, each of which may be weighted (multiplied by an appropriate factor) when combining the criteria to determine the final decision: SCS/antennas with a lower number of bit errors are preferred to SCS/antennas with a higher number of bit errors, average SNR for a given SCS/antenna must be greater than a predetermined threshold to be designated as the primary; SCS/antennas with higher
- 30 average SNR are preferred over those with lower average SNR; SCS/antennas with lower SNR variance are preferred to those with higher SNR variance; and SCS/antennas with a faster SNR rate of change at the on-set of the transmission are preferred to those

with a slower rate of change. The weighting applied to each of these criteria may be adjusted by the operator of the Wireless Location System to suit the particular design of each system.

- 5 The candidate list of SCS's 10 and antennas 10-1 are selected using a predetermined set of criteria based, for example, upon knowledge of the types of cell sites, types of antennas at the cell sites, geometry of the antennas, and a weighting factor that weights certain antennas more than other antennas. The weighting factor takes into account knowledge of the terrain in which the Wireless Location System is operating, past
- 10 empirical data on the contribution of each antenna has made to good location estimates, and other factors that may be specific to each different WLS installation. In one embodiment, for example, the Wireless Location System may select the candidate list to include all SCS's 10 up to a maximum number of sites (`max_number_of_sites`) that are closer than a predefined maximum radius from the primary site
- 15 (`max_radius_from_primary`). For example, in an urban or suburban environment, wherein there may be a large number of cell sites, the `max_number_of_sites` may be limited to nineteen. Nineteen sites would include the primary, the first ring of six sites surrounding the primary (assuming a classic hexagonal distribution of cell sites), and the next ring of twelve sites surrounding the first ring. This is depicted in Figure 9. In
- 20 another embodiment, in a suburban or rural environment, `max_radius_from_primary` may be set to 40 miles to ensure that the widest possible set of candidate SCS/antennas is available. The Wireless Location System is provided with means to limit the total number of candidate SCS's 10 to a maximum number (`max_number_candidates`), although each candidate SCS may be permitted to choose the best port from among its
- 25 available antennas. This limits the maximum time spent by the Wireless Location System processing a particular location. `Max_number_candidates` may be set to thirty-two, for example, which means that in a typical three sector wireless communications system with diversity, up to $32 * 6 = 192$ total antennas could be considered for location processing for a particular transmission. In order to limit the time spent processing a
- 30 particular location, the Wireless Location System is provided with means to limit the number of antennas used in the location processing to `max_number_antennas_processed`.

Max_number_antennas_processed is generally less than max_number_candidates, and is typically set to sixteen.

While the Wireless Location System is provided with the ability to dynamically
5 determine the candidate list of SCS's 10 and antennas based upon the predetermined set of criteria described above, the Wireless Location System can also store a fixed candidate list in a table. Thus, for each cell site and sector in the wireless communications system, the Wireless Location System has a separate table that defines the candidate list of SCS's 10 and antennas 10-1 to use whenever a wireless transmitter
10 initiates a transmission in that cell site and sector. Rather than dynamically choose the candidate SCS/antennas each time a location request is triggered, the Wireless Location System reads the candidate list directly from the table when location processing is initiated.

15 In general, a large number of candidate SCS's 10 is chosen to provide the Wireless Location System with sufficient opportunity and ability to measure and mitigate multipath. On any given transmission, any one or more particular antennas at one or more SCS's 10 may receive signals that have been affected to varying degrees by multipath. Therefore, it is advantageous to provide this means within the Wireless
20 Location System to dynamically select a set of antennas which may have received less multipath than other antennas. The Wireless Location System uses various techniques to mitigate as much multipath as possible from any received signal; however it is frequently prudent to choose a set of antennas that contain the least amount of multipath.

25 Choosing Reference and Cooperating SCS/Antennas

In choosing the set of SCS/antennas to use in location processing, the Wireless Location System orders the candidate SCS/antennas using several criteria, including for example: average SNR over the transmission interval used for location processing, the variance in the SNR over the same interval, correlation of the beginning of the received
30 transmission against a pure pre-cursor (i.e. for AMPS, the dotting and Barker code) and/or demodulated data from the primary SCS/antenna, the time of the on-set of the transmission relative to the on-set reported at the SCS/antenna at which the transmission

was demodulated, and the magnitude and rate of change of the SNR from just before the on-set of the transmission to the on-set of the transmission, as well as other similar parameters. The average SNR is typically determined at each SCS, and for each antenna in the candidate list either over the entire length of the transmission to be used for location processing, or over a shorter interval. The average SNR over the shorter interval can be determined by performing a correlation with the dotting sequence and/or Barker code and/or sync word, depending on the particular air interface protocol, and over a short range of time before, during, and after the timestamp reported by the primary SCS 10. The time range may typically be +/- 200 microseconds centered at the timestamp, for example. The Wireless Location System will generally order the candidate SCS/antennas using the following criteria, each of which may be weighted when combining the criteria to determine the final decision: average SNR for a given SCS/antenna must be greater than a predetermined threshold to be used in location processing; SCS/antennas with higher average SNR are preferred over those with lower average SNR; SCS/antennas with lower SNR variance are preferred to those with higher SNR variance; SCS/antennas with an on-set closer to the on-set reported by the demodulating SCS/antenna are preferred to those with an on-set more distant in time; SCS/antennas with a faster SNR rate of change are preferred to those with a slower rate of change; SCS/antennas with lower incremental weighted GDOP are preferred over those with higher incremental weighted GDOP, wherein the weighting is based upon estimated path loss from the primary SCS. The weighting applied to each of these preferences may be adjusted by the operator of the Wireless Location System to suit the particular design of each system. The number of different SCS's 10 used in the location processing is maximized up to a predetermined limit; the number of antennas used at each SCS 10 is limited to a predetermined limit; and the total number of SCS/antennas used is limited to max_number_antennas_processed. The SCS/antenna with the highest ranking using the above described process is designated as the reference SCS/antenna for location processing.

30 Best Port Selection Within an SCS 10

Frequently, the SCS/antennas in the candidate list or in the list to use in location processing will include only one or two antennas at a particular SCS 10. In these cases,

the Wireless Location System may permit the SCS 10 to choose the “best port” from all or some of the antennas at the particular SCS 10. For example, if the Wireless Location System chooses to use only one antenna at a first SCS 10, then the first SCS 10 may select the best antenna port from the typical six antenna ports that are connected to that SCS 10, or it may choose the best antenna port from among the two antenna ports of just one sector of the cell site. The best antenna port is chosen by using the same process and comparing the same parameters as described above for choosing the set of SCS/antennas to use in location processing, except that all of the antennas being considered for best port are all in the same SCS 10. In comparing antennas for best port, the SCS 10 may also optionally divide the received signal into segments, and then measure the SNR separately in each segment of the received signal. Then, the SCS 10 can optionally choose the best antenna port with highest SNR either by (i) using the antenna port with the most segments with the highest SNR, (ii) averaging the SNR in all segments and using the antenna port with the highest average SNR, or (iii) using the antenna port with the highest SNR in any one segment.

Detection and Recovery From Collisions

Because the Wireless Location System will use data from many SCS/antenna ports in location processing, there is a chance that the received signal at one or more particular SCS/antenna ports contains energy that is co-channel interference from another wireless transmitter (i.e. a partial or full collision between two separate wireless transmissions has occurred). There is also a reasonable probability that the co-channel interference has a much higher SNR than the signal from the target wireless transmitter, and if not detected by the Wireless Location System, the co-channel interference may cause an incorrect choice of best antenna port at an SCS 10, reference SCS/antenna, candidate SCS/antenna, or SCS/antenna to be used in location processing. The co-channel interference may also cause poor TDOA and FDOA results, leading to a failed or poor location estimate. The probability of collision increases with the density of cell sites in the host wireless communications system, especially in dense suburban or rural environments where the frequencies are re-used often and wireless usage by subscribers is high.

Therefore, the Wireless Location System includes means to detect and recover from the types of collisions described above. For example, in the process of selecting a best port, reference SCS/antenna, or candidate SCS/antenna, the Wireless Location System determines the average SNR of the received signal and the variance of the SNR over the
5 interval of the transmission; when the variance of the SNR is above a predetermined threshold, the Wireless Location System assigns a probability that a collision has occurred. If the signal received at an SCS/antenna has increased or decreased its SNR in a single step, and by an amount greater than a predetermined threshold, the Wireless Location System assigns a probability that a collision has occurred. Further, if the
10 average SNR of the signal received at a remote SCS is greater than the average SNR that would be predicted by a propagation model, given the cell site at which the wireless transmitter initiated its transmission and the known transmit power levels and antenna patterns of the transmitter and receive antennas, the Wireless Location System assigns a probability that a collision has occurred. If the probability that a collision has occurred is
15 above a predetermined threshold, then the Wireless Location System performs the further processing described below to verify whether and to what extent a collision may have impaired the received signal at an SCS/antenna. The advantage of assigning probabilities is to reduce or eliminate extra processing for the majority of transmissions for which collisions have not occurred. It should be noted that the threshold levels,
20 assigned probabilities, and other details of the collision detection and recovery processes described herein are configurable, i.e., selected based on the particular application, environment, system variables, etc., that would affect their selection.

For received transmissions at an SCS/antenna for which the probability of a collision is
25 above the predetermined threshold and before using RF data from a particular antenna port in a reference SCS/antenna determination, best port determination or in location processing, the Wireless Location System preferably verifies that the RF data from each antenna port is from the correct wireless transmitter. This is determined, for example, by demodulating segments of the received signal to verify, for example, that the MIN,
30 MSID, or other identifying information is correct or that the dialed digits or other message characteristics match those received by the SCS/antenna that initially demodulated the transmission. The Wireless Location System may also correlate a short

- segment of the received signal at an antenna port with the signal received at the primary SCS 10 to verify that the correlation result is above a predetermined threshold. If the Wireless Location System detects that the variance in the SNR over the entire length of the transmission is above a pre-determined threshold, the Wireless Location System may
- 5 divide the transmission into segments and test each segment as described herein to determine whether the energy in that segment is primarily from the signal from the wireless transmitter for which location processing has been selected or from an interfering transmitter.
- 10 The Wireless Location System may choose to use the RF data from a particular SCS/antenna in location processing even if the Wireless Location System has detected that a partial collision has occurred at that SCS/antenna. In these cases, the SCS 10 uses the means described above to identify that portion of the received transmission which represents a signal from the wireless transmitter for which location processing has been
- 15 selected, and that portion of the received transmission which contains co-channel interference. The Wireless Location System may command the SCS 10 to send or use only selected segments of the received transmission that do not contain the co-channel interference. When determining the TDOA and FDOA for a baseline using only selected segments from an SCS/antenna, the Wireless Location System uses only the
- 20 corresponding segments of the transmission as received at the reference SCS/antenna. The Wireless Location System may continue to use all segments for baselines in which no collisions were detected. In many cases, the Wireless Location System is able to complete location processing and achieve an acceptable location error using only a portion of the transmission. This inventive ability to select the appropriate subset of the
- 25 received transmission and perform location processing on a segment by segment basis enables the Wireless Location System to successfully complete location processing in cases that might have failed using previous techniques.

Multiple Pass Location Processing

- 30 Certain applications may require a very fast estimate of the general location of a wireless transmitter, followed by a more accurate estimate of the location that can be sent subsequently. This can be valuable, for example, for E9-1-1 systems that handle wireless

calls and must make a call routing decision very quickly, but can wait a little longer for a more exact location to be displayed upon the E9-1-1 call-taker's electronic map terminal. The Wireless Location System supports these applications with an inventive multiple pass location processing mode.

5

In many cases, location accuracy is enhanced by using longer segments of the transmission and increasing the processing gain through longer integration intervals. But longer segments of the transmission require longer processing periods in the SCS 10 and TLP 12, as well as longer time periods for transmitting the RF data across the communications interface from the SCS 10 to the TLP 12. Therefore, the Wireless Location System includes means to identify those transmissions that require a fast but rough estimate of the location followed by more complete location processing that produces a better location estimate. The Signal of Interest Table includes a flag for each Signal of Interest that requires a multiple pass location approach. This flag specifies the maximum amount of time permitted by the requesting location application for the first estimate to be sent, as well as the maximum amount of time permitted by the requesting location application for the final location estimate to be sent. The Wireless Location System performs the rough location estimate by selecting a subset of the transmission for which to perform location processing. The Wireless Location System may choose, for example, the segment that was identified at the primary SCS/antenna with the highest average SNR. After the rough location estimate has been determined, using the methods described earlier, but with only a subset of the transmission, the TLP 12 forwards the location estimate to the AP 14, which then forwards the rough estimate to the requesting application with a flag indicating that the estimate is only rough. The Wireless Location System then performs its standard location processing using all of the aforementioned methods, and forwards this location estimate with a flag indicating the final status of this location estimate. The Wireless Location System may perform the rough location estimate and the final location estimate sequentially on the same DSP in a TLP 12, or may perform the location processing in parallel on different DSP's. Parallel processing may be necessary to meet the maximum time requirements of the requesting location applications. The Wireless Location System supports different maximum time requirements from different location applications for the same wireless transmission.

Very Short Baseline TDOA

The Wireless Location System is designed to operate in urban, suburban, and rural areas. In rural areas, when there are not sufficient cell sites available from a single wireless carrier, the Wireless Location System can be deployed with SCS's 10 located at the cell sites of other wireless carriers or at other types of towers, including AM or FM radio station, paging, and two-way wireless towers. In these cases, rather than sharing the existing antennas of the wireless carrier, the Wireless Location System may require the installation of appropriate antennas, filters, and low noise amplifiers to match the frequency band of the wireless transmitters of interest to be located. For example, an AM radio station tower may require the addition of 800 MHz antennas to locate cellular band transmitters. There may be cases, however, wherein no additional towers of any type are available at reasonable cost and the Wireless Location System must be deployed on just a few towers of the wireless carrier. In these cases, the Wireless Location System supports an antenna mode known as very short baseline TDOA. This antenna mode becomes active when additional antennas are installed on a single cell site tower, whereby the antennas are placed at a distance of less than one wavelength apart. This may require the addition of just one antenna per cell site sector such that the Wireless Location System uses one existing receive antenna in a sector and one additional antenna that has been placed next to the existing receive antenna. Typically, the two antennas in the sector are oriented such that the primary axes, or line of direction, of the main beams are parallel and the spacing between the two antenna elements is known with precision. In addition, the two RF paths from the antenna elements to the receivers in the SCS 10 are calibrated.

25

In its normal mode, the Wireless Location System determines the TDOA and FDOA for pairs of antenna that are separated by many wavelengths. For a TDOA on a baseline using antennas from two different cell sites, the pairs of antennas are separated by thousands of wavelengths. For a TDOA on a baseline using antennas at the same cell site, the pairs of antennas are separated by tens of wavelengths. In either case, the TDOA determination effectively results in a hyperbolic line bisecting the baseline and passing through the location of the wireless transmitter. When antennas are separated by multiple

30

wavelengths, the received signal has taken independent paths from the wireless transmitter to each antenna, including experiencing different multipath and Doppler shifts. However, when two antennas are closer than one wavelength, the two received signals have taken essentially the same path and experienced the same fading, multipath, and Doppler shift. Therefore, the TDOA and FDOA processing of the Wireless Location System typically produces a Doppler shift of zero (or near-zero) hertz, and a time difference on the order of zero to one nanosecond. A time difference that short is equivalent to an unambiguous phase difference between the signals received at the two antennas on the very short baseline. For example, at 834 MHz, the wavelength of an AMPS reverse control channel transmission is about 1.18 feet. A time difference of 0.1 nanoseconds is equivalent to a received phase difference of about 30 degrees. In this case, the TDOA measurement produces a hyperbola that is essentially a straight line, still passing through the location of the wireless transmitter, and in a direction that is rotated 30 degrees from the direction of the parallel lines formed by the two antennas on the very short baseline. When the results of this very short baseline TDOA at the single cell site are combined with a TDOA measurement on a baseline between two cell sites, the Wireless Location System can determine a location estimate using only two cell sites.

Monitoring of Call Information

Overview

A network-based WLS uses geographically separated receivers to listen for signals from a roving transmitter. In a wireless communications network, the roving transmitter, in this case a wireless phone, can be broadcasting on any one of potentially thousands of control or traffic channels. A mechanism is needed for collecting this channel and caller information. We will now describe the subject invention, which provides a mechanism for communicating with the wireless system with minimal impact to the existing system by passively monitoring a specific link for cell ID, timing advance or PN offset, frequency, caller information and other information specific to a subscriber. (This is alluded to above in connection with the description of the AP – see the subsection titled "Monitor Internal Wireless Communications System Interfaces, State Table.") The specific link, e.g., may be the BSC-BTS link called the "Abis" link in GSM and other names by various manufacturers for other radio access system (AMPS,

CDMA, TDMA, PDC, J-CDMA, CDMAOne, CDMA2000, W-CDMA, etc.). This information obtained from the link is passed to a TDOA, AOA, or hybrid TDOA/AOA - based location system that uses the information to acquire and process wireless phone signals for the purposes of location estimation.

5

Figure 10 schematically depicts a system in which a Base Transceiver Site (BTS) 10-1 is coupled to a Base Station Controller (BSC) 10-3 by way of an Abis interface. As shown, an Abis monitor 10-2 is coupled to the Abis interface. This aspect of the present invention is described in greater detail below. Figure 10 further depicts a Mobile

10 Switching Center (MSC) 10-4 coupled to the BSC via an "A interface", as well as a Visitor Location Register (VLR) 10-5 and Home Location Register (HLR) 10-6. The BTS, BSC, MSC, VLR and HLR are well known components of a GSM wireless communications system.

15 The present invention, in a presently preferred implementation, provides a mobile station (MS) management method for a WLS that is overlaid on at least a portion of a wireless communications system. The wireless communications system, as indicated above, includes BTS equipment connected to BSC equipment. The inventive method is generally illustrated by the flowchart of Figure 11, and involves:

- 20 monitoring the communications between at least one BTS and at least one BSC (step S110);
- extracting MS information from the monitored communications (step S112);
- forwarding the extracted MS information to the WLS (step S114);
- the WLS may then use the extracted MS information for a variety of purposes (step
- 25 S116), which are outlined below.

The extracted MS information may include the mobile station identification (MSID), the called number dialed by the user of the MS, the contents of messages sent to the MS or from the MS, or frequency assignment information sent to the MS. In addition, the

30 extracted MS information may include any of the following presently in use by the MS: the control channel, the traffic channel, the mobile directory number (MDN), the Electronic Serial Number (ESN), the Mobile Identity Number (MIN), the Mobile

Subscriber Identification (MSI), the international mobile subscriber identity (IMSI), the temporary mobile subscriber identity (TMSI), or the mobile station international ISDN number (MSISDN).

- 5 As mentioned, there are a number of different uses for the extracted information. First, the WLS may use the extracted information to determine whether to perform location processing for the MS, or to determine which radio resources to use in performing location processing for the MS. In addition, the WLS may store the extracted MS information in a database for use at a later time or by other applications. Preferably, the
- 10 WLS will remove the extracted MS information from the database after it is no longer valid. For example, the extracted MS information may be determined to be no longer valid because the MS is no longer registered with the wireless communications system, because a predetermined period of time has expired, because a predetermined period of time has expired without an update to the extracted MS information, or because the
- 15 extracted MS information does not match any of a set of predetermined criteria. The set of predetermined criteria may include information about the identity of the MS or the number called by the user of the MS.

Detailed Description of Exemplary Embodiment for Abis Monitoring

20 1. Introduction

A method to employ a location system of the kind described above to locate GSM mobile phones will now be described. With the architecture described herein, the WLS would not be required to detect and demodulate messages from the mobile terminal during call setup. Instead, the location system would derive call setup information from

25 the Abis interface between the BTS and the BSC. From the Abis interface, the location system can identify the calling party (indirectly), the called party (i.e., 911), and the TDMA/FDMA resource that is being used for a given call at any time. In the following sections, an overview of call setup in a GSM system will be presented, including relevant messages and formats. Next, an exemplary architecture for identifying and locating calls

30 in a GSM system is presented, followed by the high level subsystem features used to locate GSM calls.

2. Mobile Originated Call Setup in a GSM System

2.1. Call Setup-- Early Stages

The following discussion assumes that the mobile station (MS) is in the state of
5 being "normally registered" with the network. An overview of the transactions involved
in call setup emphasizing the function of the different protocol layers is presented in
Figure 12A. It should be understood that some of the layers are completely internal to
one physical subsystem, e.g., the MS, and are used more for conceptual clarification.

10 2.1.1 Channel Request

When the MS desires to originate a call, presumably a "911" call, the CC layer in
the handset presents a request to the MM layer therein, which in turn asks the Radio
Resource (RR) layer, or Layer 3, to request a radio connection. This is depicted in the top
flow line of Figure 12A. This request is transparent to the link layer (Layer 2) and is
15 simply viewed by it as a "data indication" to be transported to higher layers.

This channel request on the physical layer (Layer 1), however, has a unique format. It
uses the "Access Burst" which is a shorter burst than the regular burst. The access burst
consists of 87 channel bits, rather than the regular 147 bits, with the remainder as guard
20 time. The MS needs the extra guard time because time advance as measured and
provided to the MS by the BTS is not available on the very first instance of random
access.

The channel request message consists of only 8 information bits. These are then coded
25 with a combination of a rate $\frac{1}{2}$ convolutional code and a 6-parity-bits cyclic code to yield
a 36-bit block. This, in turn, is augmented with a 41 bit unique training sequence, and tail
bits in the beginning and the end to create the 87-bit access burst shown in Figure 12B.

The 8 information bits in the RR layer channel request message take the form shown in
30 Figure 12C. The coding scheme for the Channel Request message is defined in
paragraph 4.6 of GSM 05.03.

The random reference is an unformatted field of variable length between two and five bits long. It is used to distinguish responses from the BTS to mobiles that may have requested radio channels simultaneously. The Establishment Cause field is also of variable length, between 3 and 6 bits long, with the generic cause of requesting a radio link. Some of the bit sequences of particular interest in this field are shown in Table 2-1, below.

Table 2-1. Some of the Channel Request Causes and their Bit Sequences (see Section 9.1.8/GSM 04.08)

Message	Establishment Cause
101xxxxx	Emergency call
111xxxxx	Originating call and TCH/F (full rate traffic channel) needed, etc.
0000xxxx	Location Updating
110xxxxx	Call re-establishment, etc.
100xxxxx, 0010xxxx 0011xxxx, 0001xxxx	Answers to paging
...	Others

As can be seen, an emergency call, whatever that is defined to be by the carrier, and whatever the handset software implements accordingly, has a unique bit pattern that could be detected. The channel request is demodulated in the BTS and passed on, in a transparent manner, via a Layer 2 "data indication" to the BSC, as a Channel Required message. The format of Channel Required message is shown in Table 2-2.

Table 2-2. Channel Required Message on the Abis Interface (Section 8.5.3/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Request Reference	9.3.19	M	TV	4
Access Delay	9.3.17	M	TV	2
Physical Context	9.3.16	O 1)	TLV	>=2

1) Optional element for additional physical channel information.

The most interesting fields here are those of the Request Reference. These are shown in more detail in Figure 12D. The RA octet is the key information octet sent by the MS in the Channel Request and would contain the random identifier and the establishment cause, e.g., bit pattern 101 for 911. The other octets contain the coding of the absolute
5 frame number modulo 42432 in which the access burst was received.

The other contents of the Channel Required message on the Abis Interface are the access delay measured by the BTS (on the access burst), and the channel number. The frame number and access delay can be used by the location system to determine the frame
10 epoch relative to GPS time, as will be explained later. All of the useful information provided by the Channel Request message on the air interface can be obtained from the Request Reference field of the Channel Required message on the Abis interface.

2.1.2 Immediate Assignment

15 Once the Channel Required message is received and processed by the BSC, it responds by activating the appropriate transceiver at the BTS to carry the SDCCH signaling channel. This is performed via the Channel Activation command. The Channel Activation command has the format and contents shown in Table 2-3 below.

20 The mandatory information in the Channel Activation command includes the Channel Number, the Activation Type, and the Channel Mode. The activation type specifies whether it is an immediate assignment or a normal assignment, a handoff, or an additional assignment (e.g., for multi-slot operation). The channel mode is of variable length and contains detailed information on the mode of the channel, i.e., speech, data or
25 signaling, its rate, speech coding algorithm, and DTX on or off.

Another information element in the Channel Activation command is the Encryption Information. This information is included only if ciphering is to be applied by the BTS, hence would be normally included in the command. The encryption information element
30 is depicted in Figure 12F. Not only does it include the algorithm but also the key (K_c) to be used for the ciphering and deciphering operations.

More information to the radio devices is provided in the Channel Activation command, including BS and MS power settings and parameters, and the timing advance.

- When the BSC receives a positive acknowledgement from the BTS via the Channel
- 5 Activation Acknowledge message it sends the Immediate Assign Command to the BTS. This is used by the BTS to create the Immediate Assignment message, which is scheduled for transmission by the BTS. The Immediate Assign Command on the Abis Interface contains the complete radio definition of the physical signaling channel assigned.

10

Table 2-3. Channel Activation Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Activation Type	9.3.3	M	TV	2
Channel Mode	9.3.6	M	TLV	8-9
Channel Identification	9.3.5	O 7)	TLV	8
Encryption information	9.3.7	O 1)	TLV	>=3
Handover Reference	9.3.9	C 2)	TV	2
BS Power	9.3.4	O 3)	TV	2
MS Power	9.3.13	O 3)	TV	2
Timing Advance	9.3.24	C 3) 4)	TV	2
BS Power Parameters	9.3.32	O 5)	TLV	>=2
MS Power Parameters	9.3.31	O 5)	TLV	>=2
Physical Context	9.3.16	O 6)	TLV	>=2
SACCH Information	9.3.29	O 8)	TLV	>=3
UIC	9.3.50	C 9)	TLV	3

- 1) The Encryption Information element is only included if ciphering is to be applied.
- 2) The Handover Reference element is only included if activation type is handover.
- 3) If BS Power, MS Power and/or Timing Advance elements are present, they are to be used to set the initial transmission power and the initial L1-header.
- 4) The Timing Advance element must be included if activation type is intra cell channel change.
- 5) The BS and MS Power Parameters elements are included to indicate that BS and/or MS power control is to be performed by BTS. The maximum power to be used is indicated in the BS and MS Power elements respectively.
- 6) Optional element for additional physical channel information.
- 7) Included if compatibility with phase1 is required.

Table 2-4. Channel Activation Acknowledge (Section 8.4.2/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Frame number	9.3.8	M	TV	3

5 Table 2-5. Immediate Assign Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Full Imm. Assign Info	9.3.35	M	TV	25

10 The Immediate Assign Command also contains the Channel Number Information Element, as shown. The Channel Number contains the Channel Type, subchannel number, and the TN for all messages sent across the Abis interface. This allows correlation of an Abis message with the air interface message. The BTS sends the corresponding Layer 3 Immediate Assignment command to the MS somewhere on the CCCH. The MS needs to listen to both the CCCH and the BCCH during that period.

15

The Immediate Assignment message causes the mobile to seize the dedicated signaling channel on which it will exchange subsequent signaling messages pertaining to call setup. There are two varieties in the specification for this message. The usual Immediate Assignment, and an Immediate Assignment Extended version, which addresses
20 simultaneously two mobile stations in the same cell and provides them their dedicated signaling channel information.

For the purposes of this discussion, examining the Immediate Assignment message will suffice. (If needed in the future, the extended message version can be found in the section 9.1.19 /GSM 04.08.)

- 5 There are many important fields in the Immediate Assignment message. The "Immediate Assignment Message Type" field is just the octet: 00111111. (There are other patterns for assignment extended and rejected.) The 3-octet request reference contains first the exact content of the channel request and the rest enables the computation of the frame number (modulo 42432) in which the request was received. The channel description
- 10 contains of course critical RF information.

Table 2-6. The Radio Resource Immediate Assignment Message to the Mobile (Section 9.1.18/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
7C	L2 Pseudo Length	10.5.2.19	M	V	1
	RR management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Immediate Assignment Message Type	10.4	M	V	1
	Page Mode	10.5.2.26	M	V	1/2
	Spare Half Octet	10.5.1.8	M	V	1/2
	Channel Description	10.5.2.5	M	V	3
	Request Reference	10.5.2.30	M	V	3
	Timing Advance	10.5.2.40	M	V	1
	Mobile Allocation	10.5.2.21	M	LV	1-9
	Starting Time	10.5.2.38	O	TV	3
	IA Reset Octets (frequency parameters, before time)	10.5.2.16	M	V	0-11

15

Notes: M = Mandatory; O = Optional; V = Value; T = Type; L = Length (octet)

- In Figure 12H, TN is the timeslot number (0 to 7), TSC is the training sequence (0 to 7,
- 20 and H is the hopping indicator bit. If H = 0, no hopping is used and ARFCN is the Absolute Radio Frequency Channel Number coded in binary (0 – 1023). If H =1, then the hopping sequence is defined by MAIO (the Mobile Allocation Index Offset), and

(HSN the hopping sequence number), which takes the values 0 –63. The Mobile Allocation field and the IA rest Octets also relate to frequency hopping.

5 The Channel Description information element is defined for the Immediate Assignment message. The similarity between the Channel Description IE of the air interface and the Channel Number of the Abis messages allows correlation of Abis messages with specific physical channels on the air interface.

10 The timing advance field is a binary coded representation of the advance in bit periods required of the MS according to the measurement performed at the BTS of the received random access burst. The MS transmissions are always 3 regular burst periods behind the BTS transmission offset by the time advance specified by the BTS.

The optional starting time is again in TDMA FN units (modulo 42432). The frame is approximately 4.615 ms (8 bursts).

15 The Immediate Assign command on the Abis Interface contains the Immediate Assign message to be transmitted on the air interface. Thus, it contains three very key information elements related to a 911 call in the immediate assignment: the Request Reference (containing the bit pattern corresponding to emergency call), the Channel
20 Description, and the Mobile Allocation. This is all the information the location system needs to track the signaling channel used during the setup process of a 911 call.

2.1.3. CM Service Request

25 Once the MS receives the Immediate Assignment from the BTS, it adjusts its radio and aligns its timing then transmits back to the BTS on the specified dedicated (logical) channel the Connection Management (CM) Service Request. (That assumes, as mentioned earlier, that the MS was in the proper registered idle state). The CM service request message is synthesized and stored in the handset when the caller initiates the call sequence.

30 At the link layer, the CM service request is carried inside the SABM (Set Asynchronous Balanced Mode) Layer –2 frame, which basically enables the exchange and

acknowledgment of MS-unique information between the MS and BTS, thus avoiding any potential MS ambiguity during the random access contention phase. First, the CM service request message contains important information that can be very useful to an E-911 location system.

5

Table 2-7. Contents of the CM Service Request Message from the MS (Table 9.45/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Mobility Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	CM Service Request Message Type	10.4	M	V	1
	CM Service Type	10.5.3.3	M	V	1/2
	Ciphering Key Sequence Number	10.5.1.2	M	V	1/2
	Mobile Station Classmark	10.5.1.6	M	LV	4
	Mobile Identity	10.5.1.4	M	LV	2-9

10

The CM service request message type octet belongs to the family of mobility management message types and is 0x100100. The CM Service Type half octet carries information that could of key importance to an E-911 location system. The half byte structure and content is shown in Figure 12I.

15

The half octet pertaining to the ciphering key sequence number contain three bits that provide the network with one of seven possible sequence numbers for, or a 111 pattern which indicates that no key is present in the MS.

20 The MS "classmark 2" message is depicted in Figure 12J. It carries information on maximum RF power capability of the MS: The MS classmark 2 message also carries information on the encryption algorithm A5/x the MS supports (if any). The length of the message is variable and varies up to four octets total (only L and V are transmitted).

Finally, the important mobile identity fields are transmitted to conclude the CM Service request message from the MS. There are three types of MS identity that could be used.

These are:

- 5 TMSI: Temporary Mobile Subscriber Identity;
- IMSI: International Mobile Subscriber Identity; and
- IMEI: International Mobile Station Equipment Identity.

Relaying this information to the network is done through the Mobile Identity fields, which can be 2 to 9 octets long, and are illustrated in Figure 12K. The type of MS
10 identity used is provided in octet 3.

There are certain rules in the specification on the use of the different identity types available. For mobile originating calls, for other than "emergency" call establishment or re-establishment the priority will be for the MS to use:

- 1 TMSI if available,
- 15 2. IMSI if no TMSI is available.

In the case of emergency call establishment or re-establishment, a third priority is added:

- 3. IMEI is used if neither a TMSI nor an IMSI is available, or if there is no SIM, or the MS does not consider the SIM valid.

20 The actual coding of the IMSI or IMEI can be found in the specification in Section 10.5.1.4/GSM 04.08.

When the CM Service Request message (carried in the SABM frame) is received at he
25 BTS, it is sent back to the MS without any modification but encapsulated inside a UA (Unnumbered acknowledgement) frame. This takes place on the DCCH radio channel specified earlier in the Immediate Assignment.

The BTS simultaneously passes the CM Service Request to the BSC in an RR Establish
30 Indication message over the Abis interface. The particulars (e.g., radio attributes) of the mobile are stored in the BTS and/or BSC for later use. The Establishment Indication can be identified as an SDCCH message by the link Identifier. The BSC at this point establishes an SCCP (Signal Connection Control Part) connection on the A-Interface to the MSC. The CM Service Request message may be optionally piggybacked on the

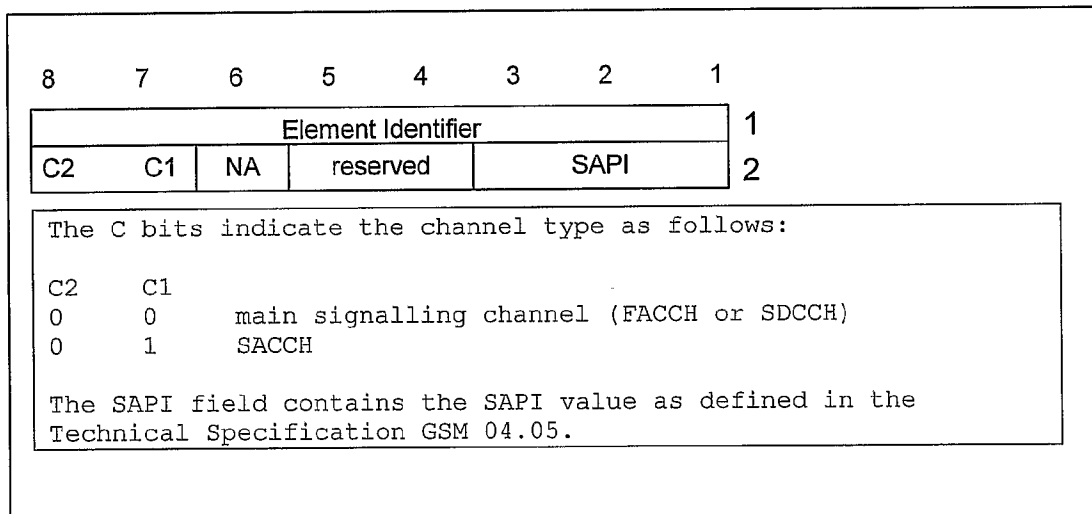
SCCP Connection Request message. It may also be sent after the SCCP connection establishment via a BSSMAP Complete Layer 3 Information message.

5 Table 2-9. Establishment Indication Message Carrying the Service Request on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Link Identifier	9.3.2	M	TV	2
L3 Information	9.3.11	O 1)	TLV	3-23

- 1) The L3 Information field is present only if the SABM frame contained a non-empty information field.

Table 2-10 Link Identifier Information Element (Section 9.3.2/GSM 08.58)



- Now, after being informed by the BSC of the existing service request, which contains the
- 10 mobile subscriber's specifics, the MSC becomes involved and has the information to trigger the actions in the upper layers (MM and CC). The MSC now takes charge of the ensuing characteristics of the RR session and initiates the appropriate steps of authentication, encryption, call routing, and so on. Because the full CM Service Request message is sent across the Abis interface, the calling party's identity can be obtained
- 15 from the Abis interface.

2.2 Authentication

The previous section has dealt with the early phase of call set-up, mostly that of radio resource assignment. The protocol layers involved are 1 through 3: physical, data
 5 link, and radio resource link. Before a call setup can go further, certain verification/security procedures need to be executed and these generally belong to the class of mobility management. This can be thought of as Layer 4 of the protocol stack.

The network may trigger the authentication of the PCS user identity when the user
 10 applies for:

- a change of a subscriber-related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service),
- an access to a service (including some or all of: set-up of mobile originating or
 15 terminated calls, activation or deactivation of a supplementary service), or
- first network access after restart of MSC/VLR, or in the event of cipher key sequence number mismatch.

The authentication procedure includes the following exchange between the network and
 20 the MS. The Network transmits and Authentication Request Message. The user terminal performs some computation and replies with the Authentication Response Message shown in Table 2-12.

Table 2-12. Authentication Response Message Contents

25

IEI	Information Element	Reference	Presence	Format	Length
	Mobility Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Authentication Response Message Type	10.4	M	V	1
	Authentication parameter SRES	10.5.3.2	M	V	4

2.3 Encryption/Ciphering

Although the subscriber identity and dialed digits can be determined from the Abis interface, it may be required for the location system to be able to recreate the channel bits transmitted by the mobile terminal for station based location processing. In order to create bits transmitted by the mobile, the location system may need to know of the encryption algorithm, key, and synchronization. To maintain the confidentiality of signaling and user data over the radio link, four items may have to be specified: encryption method; key setting; starting of the encryption and decryption processes; and synchronization. The encryption algorithm is known as A5.

10 Mutual key setting is the procedure that allows the MS and the network to agree on the key Kc to be used in the encryption and decryption algorithm A5. Key setting is triggered by the authentication procedure. A key setting must occur on a DCCH not yet encrypted and as soon as the identity of the mobile user (TMSI or IMSI) is known by the network.

15 Because of the potential inconsistencies that could exist between the "current" Kc on the MS and network sides, the parameter Ciphering Key Sequence Number alluded to earlier is included in the location update request and CM service request. This number is stored with the Kc, if it is found to be inconsistent upon the receipt of, say, a CM service request, the MSC/VLR knows that an authentication procedure is required before ordering the ciphered mode.

Returning to the mechanics of encryption, the operation takes place just before modulation and after interleaving; symmetrically, the decryption takes place after the demodulation. The encryption and decryption start at different instances.

The ciphering and deciphering operations are performed by applying an exclusive-or operation between the 114 coded bits of a radio burst and 114-bit ciphering sequences generated by A5 as depicted in Figure 12M. The two link directions use different sequences: for each burst, one sequence is used for ciphering in the MS and deciphering in the BTS, whereas another is used for ciphering at the BTS and deciphering at the MS.

The use of the frame number guarantees the required synchronization of the operations. For all types of radio channels the frame number changes from burst to burst. Accordingly, each burst of a given communication in the same direction uses a different ciphering sequence. The successive values for the frame number depends on the time organization of each channel and are not necessarily consecutive.

Upon receiving the contents of the CM service request at the MSC, it initiates the procedures of authentication and ciphering. Assuming successful authentication, the MSC is now ready to start the transition of the link to the ciphered mode. Ciphering, however, is a transmission function and is performed at the BTS. The decision at the MSC therefore results in a cascade of commands and steps to execute the transition. This is illustrated in Figure 12N.

The MSC sends to the BSC a BSSMAP Cipher Mode Command on the A Interface. At the BSC the cipher mode command is encapsulated in an Encryption Command on the Abis interface. This is a non-transparent command, which contains in addition to the cipher mode command, information on the specific radio channel and the ciphering key.

Table 2-13. Encryption Command on the Abis Interface

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Encryption information	9.3.7	M	TLV	>=3
Link Identifier	9.3.2	M	TV	2
L3 Info (CIPH MOD CMD)	9.3.11	M	TLV	6

The BTS upon receiving this encryption command executes the A5 algorithm but only on the receive side. It transmits to the MS in the clear the Ciphering Mode Command message. The cipher mode setting contains a bit to identify if ciphering is to be used and three bits to specify one of the possible A5 algorithm versions. The Cipher Response half octet contains one significant bit only; it specifies whether the MS is to include its

identity, specifically its IMEI, in the confirmation response, the Ciphering Mode Complete message. The identity is included only if the IMEI was requested.

The MS upon receiving the Ciphering Mode Command on the DCCH, runs the A5
 5 algorithm and starts both ciphering and deciphering. It sends back the Ciphering Mode Complete message in the ciphered mode. When the BTS receives this and successfully decipheres it, it turns on its ciphering for subsequent transmissions. The BTS relays the Cipher Mode Complete as a data indication on the Abis Interface to the BSC. The BSC, in turn, translates that information into a MAPBSS Cipher Mode Complete message on
 10 the A-Interface to the MSC.

2.4 Call Setup-- Late Stages

After entering the ciphering mode at its end, the MS sends on the DCCH that had been assigned from the beginning the call Setup message. This message contains many
 15 types of information and can vary considerable in size depending on the requested service. For voice telephony (the case of most interest for wireless location) it is simpler in content than for data or supplementary services. The regular call setup message will be discussed first. There is also in the specification an "Emergency Setup" message, which is significantly simpler. It will be described after the more general one. The location
 20 system needs to be able to handle both cases.

The structure of the regular setup message is provided in Table 2-14. The first category of information in the setup command pertains to the bearer service capability (voice at what rate, speech coding of what version, radio channel requirement, data or fax at what
 25 rate, synchronous data or not, transcoding, and so and so forth.) This information is contained in the fields called bearer Capability 1 and 2. At least one such field is mandatory. The MS needs to specify all voice rates and versions it is capable of supporting.

30 Table 2-14. Setup Message for Mobile Originating Call (Table 9.70a/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Call Control Protocol Discriminator	10.2	M	V	1/2

	Transaction Identifier	10.3.2	M	V	1/2
	Setup Message Type	10.4	M	V	1
D-	BC Repeat Indicator	10.5.4.22	C	TV	1
04	Bearer Capability 1	10.5.4.5	M	TLV	3-10
04	Bearer Capability 2	10.5.4.5	O	TLV	3-10
1C	Facility	10.5.4.15	O	TLV	2-?
5D	Calling Party Sub-address	10.5.4.10	O	TLV	2-23
5E	Called Party BCD Number	10.5.4.7	M	TLV	3-13
6D	Called Party Sub-address	10.5.4.8	O	TLV	2-23
D-	LLC Repeat Indicator	10.5.4.22	O	TV	1
7C	Low Layer Compatibility I	10.5.4.18	O	TLV	2-15
7C	Low Layer Compatibility II	10.5.4.18	O	TLV	2-15
D-	HLC Repeat Indicator	10.5.4.22	O	TV	1
7D	High Layer Compatibility I	10.5.4.16	O	TLV	2-5
7D	High Layer Compatibility II	10.5.4.16	O	TLV	2-5
7E	User-user	10.5.4.25	O	TLV	3-35
7F	SS Version	10.5.4.24	O	TLV	2-3
A1	CLIR Suppression	10.5.4.11a	C	T	1
A2	CLIR Invocation	10.5.4.11b	O	T	1

Since the TMSI (or IMSI) has been sent earlier to the network, the calling party BCD number is optional. The called party BCD number is mandatory. It is the very first time from the beginning of the RR setup procedure that this information has been divulged. The called BCD number is 3 to 19 octets long; its structure is depicted in Figure 12P. A called party subaddress field could also be included but not usually for voice; it varies in length between 2 and 23 octets. The other optional fields in the setup message pertain to whether the MS would like to provide additional compatibility information for the lower layers, e.g., as with some possible data or supplementary services. These will likely be missing in a voice call setup.

The "Emergency Setup" message has the structure shown in Table 2-15. Obviously it does away with much unnecessary information in the case of an emergency (911) call. There are no called and calling number fields. The bearer capability is, however, included and indicates speech with the appropriate version(s) the MS supports, and the appropriate value in the radio channel requirement field. This emergency setup message can have an overall length of as little as 5 octets and as long as 12.

Table 2-15. Emergency Call Setup message Content (Section 9.3.8/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
04	Call Control Protocol Discriminator	10.2	M	V	1/2
	Transaction Identifier	10.3.2	M	V	1/2
	Emergency Setup Message Type	10.4	M	V	1
	Bearer Capability	10.5.4.5	O	TLV	3-10

- 5 The setup message is received by the BTS and forwarded transparently to the BSC as a data indication. By obtaining this data indication from the Abis interface, the location system would have access to the called party number. The BSC in turn forwards the setup message to the MSC. The MSC examines the setup message contents and analyzes the MS's request. If for some reason it cannot accept or process the call, it sends back a
- 10 message to release the link. Assuming that the MSC will service the call, it initiates whatever it needs to perform to establish the connection on the external network side and, at the same time, sends towards the MS a Call Proceeding message.

- The Call Proceeding message passes transparently through the BSC and BTS and the
- 15 message transmitted on the air interface. This message could be as simple and short as two octets; it serves to inform the MS that the call establishment request has been received and that no more call establishment information will be accepted (for now at least). The bearer capability fields may be used in the cases when terminal adaptation is needed (generally not applicable for voice).

- 20
- At initial assignment, the transmission mode is chosen by the BSC and it includes one of the signaling only modes, in clear text. In the European GSM specification three radio assignment strategies are considered: Very Early Assignment, Early Assignment, and so-called Off-the-Air Call Setup (OACSU). In very early assignment a full rate channel is
- 25 assigned as soon as it is apparent that a voice channel is likely needed, possibly as early as the receipt of the channel request. In Early Assignment a DCCH, usually of the SDCCH/8 type, is first assigned for the duration of the signaling exchanges, and then

when it is confirmed in the setup message that a voice channel is needed, then a full rate voice radio channel is assigned. In the third strategy, OACSU, a voice radio channel is not assigned until the called party answers. This may save on radio resources but can result in the need for interim announcements after the called party answers and until the
5 radio channel is assigned.

At present, an SDCCH/8 control channel is initially assigned for signaling. More generally this could be a full rate SDCCH (basically a voice channel but in signaling mode). Subsequently, during the lifetime of the RR session, the choice of transmission
10 mode depends on the communication needs and is done by the MSC. The MSC can change the mode or channel at anytime during the RR connection, and does so via an "assignment" procedure.

In the most general case two cases exist: (1) the radio channel is to stay the same but its
15 mode is to be changed, e.g., from one type of traffic to another, and (2) a new radio channel is needed to meet the voice communication requirements. The second case is the one applicable at present. (The first case would be more consistent with Very Early Assignment.)

20 To initiate the assignment procedure, the MSC sends a BSSMAP Assignment Request message to the BSC, which performs what is sometimes called a Subsequent Assignment procedure. The BSC sends to the BTS two messages, the first is a Channel Activation command, to configure and turn on the required TRX for the new channel, and the second message is the Assignment Command to be sent on the existing DCCH. The
25 Assignment Command is used when no new time advance needs to be conveyed to the MS. With the transmission of the Assignment Command, all signaling messages not related to RR management are suspended until completion of assignment.

The Assignment Command is a transparent message as far as the BTS is concerned and
30 is sent to it as a data request. Obviously this is a key message that carries critical information if following the voice channel is of interest to the location system. However,

it also contains much additional information that is very unlikely to be encountered in the case of normal voice service, particularly emergency calls.

Important elements in the message are the description of the first channel, and the power
5 IE. The channel description fields have been described earlier, and they contain the channel type, TN, the training sequence, and either the absolute radio frequency number or the hopping sequence parameters (HSN, MAIO). The power command octet specifies the initial power of the mobile; it has five bits that specify the binary representation of the power control level (range: 1-32).

10

The Assignment Command contains a host of other options. For example, a second channel could also be described after a certain starting time. This pertains primarily to the case when the MS will have two dedicated traffic channels; it is intended for half-rate voice. The Assignment Command could also include new frequency lists for frequency
15 hopping. These fields could be quite long (up to 132 octets each) and their coding involved. Since frequency hopping is likely to be implemented in the future, those fields would also need to be decoded if voice channel tracking is desired.

When the MS receives the Assignment Command it initiates the new connection at the
20 various layers. The new voice channel is established with its associated signaling channels, the SACCH and FACCH, which are distinct from the existing (sometimes called main) signaling channel, the DCCH, in use during the call setup. The MS waits for the starting time to start the voice connection and transmission, but if the starting time had already elapsed, it starts on the voice channel immediately as a reaction.

25

Upon completing the assignment, the MS transmits back to the BTS/BSC/MSC an Assignment Complete on the main DCCH. The Assignment Complete command transmitted over the air interface. The RR cause octet is "Normal Event" and its value is 00000000.

30

Table 2-16. Assignment Command Message Contents

IEI	Information Element	Reference	Presence	Format	Length
	RR management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Assignment Command Message Type	10.4	M	V	1
	Description of the First Channel, after time	10.5.2.5	M	V	3
	Power Command	10.5.2.28	M	V	1
05	Frequency List, after time	10.5.2.13	C	TLV	4-132
62	Cell Channel Description	10.5.2.1	O	TV	17
63	Mode of the First Channel	10.5.2.6	O	TV	2
64	Description of the Second Channel, after time	10.5.2.5	O	TV	4
66	Mode of the Second Channel	10.5.2.7	O	TV	2
72	Mobile Allocation, after time	10.5.2.21	C	TLV	3-10
7C	Starting Time	10.5.2.38	O	TV	3
19	Frequency List, before time	10.5.2.13	C	TLV	4-132
1C	Description of the First Channel, before time	10.5.2.5	O	TV	4
1D	Description of the Second Channel, before time	10.5.2.5	O	TV	4
1E	Frequency channel sequence, before time	10.5.2.12	C	TV	10
21	Mobile Allocation, before time	10.5.2.21	C	TLV	3-10
9-	Cipher Mode Setting	10.5.2.9	O	TV	1

The BTS passes the assignment complete message transparently as a data indication to
 5 the BSC. The BSC relays the corresponding MAP message on the A-Interface. The MSC
 then sends an Alerting message to the MS to indicate that the called user at the fixed end
 has been alerted. This is a short message, with possible optional information that is not
 likely to be used for normal or emergency voice calls. The Alert message is another
 transparent message passed as a data request on the Abis interface. The Alert message is
 10 sent over the air. The location system will likely have no need for the alerting message.

The MSC then sends a Connect message to indicate call acceptance by the called user.
 The basic part of this message is again short but there are options that could be many
 octets long, such as the called number and subaddress. The MS stops its local alerting, if

any, of the MS subscriber and responds with a Connect Acknowledge which is the simple two octet message. Now, finally, the MS connects the speech path to the radio channel assigned to the voice and the conversation data flows. At this point, the DCCH is relinquished with an RF Channel Release sent to the BTS, and becomes available to

5 service another call setup.

Table 2-17. RF Channel Release (Section 8.4.14/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2

10 Table 2-18. RF Channel Release Ack (Section 8.4.19/GSM 08.58)

INFORMATION ELEMENT	REFERENCE	PRESENCE	FORMAT	LENGTH
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2

3. Mobile Terminated Call setup in a GSM System

15 A mobile terminated call setup in a GSM system includes the following steps:

Page from the network (Table 3-1).

Mobile terminal then responds with a Channel Request, with a response to page cause.

Immediate Assignment takes place.

20 The Page Response is transmitted once the SDCCH is assigned, instead of a CM Service Request.

Authentication followed by encryption.

Network Sends a Setup Message to the Mobile terminal (Table 3-2).

Mobile terminal replies with a Call Confirmed Message.

25 Call then completes in the same manner as a mobile originated call.

From the Abis interface, the location system can determine the identity of the called party, as well as the physical resources used by the call. This information allows the location system to identify calls of interest, and locate the mobile phone receiving that call.

5

Table 3-1. Contents of the Page Response Message from the MS (Table 9.25/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	RR Management Protocol Discriminator	10.2	M	V	1/2
	Skip Indicator	10.3.1	M	V	1/2
	Page Responset Message Type	10.4	M	V	1
	Ciphering Key Sequence Number	10.5.1.2	M	V	1/2
	Spare Half Octet	10.5.1.8	M	V	1/2
	Mobile Station Classmark	10.5.1.6	M	LV	4
	Mobile Identity	10.5.1.4	M	LV	2-9

10 Table 3-2. Setup Message for Mobile Terminating Call (Table 9.70/GSM 04.08)

IEI	Information Element	Reference	Presence	Format	Length
	Call Control Protocol Discriminator	10.2	M	V	1/2
	Transaction Identifier	10.3.2	M	V	1/2
	Setup Message Type	10.4	M	V	1
D-	BC Repeat Indicator	10.5.4.22	C	TV	1
04	Bearer Capability 1	10.5.4.5	O	TLV	3-10
04	Bearer Capability 2	10.5.4.5	O	TLV	3-10
1C	Facility	10.5.4.15	O	TLV	2-?
1E	Progress Indicator	10.5.4.21	O	TLV	4
34	Signal	10.5.4.23	O	TV	2
5C	Calling Party BCD Number	10.5.4.9	O	TLV	3-14
5D	Calling Party Sub-address	10.5.4.10	O	TLV	2-23
5E	Called Party BCD Number	10.5.4.7	O	TLV	3-13
6D	Called Party Sub-address	10.5.4.8	O	TLV	2-23
D-	LLC Repeat Indicator	10.5.4.22	O	TV	1
7C	Low Layer Compatibility I	10.5.4.18	O	TLV	2-15
7C	Low Layer Compatibility II	10.5.4.18	C	TLV	2-15
D-	HLC Repeat Indicator	10.5.4.22	O	TV	1
7D	High Layer Compatibility I	10.5.4.16	O	TLV	2-5
7D	High Layer Compatibility II	10.5.4.16	C	TLV	2-5

7E	User-user	10.5.4.25	O	TLV	3-35
----	-----------	-----------	---	-----	------

4. System Architecture for GSM

An illustrative system architecture for the location of GSM mobile phones is shown in Figure 12Q. The main modification to support GSM is the addition of a Monitoring Subsystem (AMS). The AMS monitors the signaling links on the Abis interface. A second modification is the NSS Interface System (NIS), which obtains a mapping of the TMSI to the IMSI and MSISDN for a subscriber, and can provide a subscriber the current location in the form of a short message.

10

The AMS will continuously monitor the Layer 2 LAPD signaling links on the Abis interface, for each cell in the GSM system. The AMS will monitor the LAPD frames and identify Immediate Assign Command messages. The AMS need not monitor the Channel Required messages, because all relevant information in the Channel Required message is repeated in the Immediate Assign Command. From the Immediate Assign Command, the AMS can identify emergency calls, and a description of the radio channel used for the subsequent signaling messages.

Once the Immediate Assign Command is detected, for a particular logical channel, the Abis message processor knows a new origination has occurred, and a new call record is created. The Abis processor will then look for a CM Service Request message from the channel, which will identify the mobile subscriber. The raw bits and the mobile identity are appended to the call record. The AMS then sends an origination indicator message with a hash code to the TLP, and the TLP then sends a TDOA data request to the appropriate SCSs with the same hash code, for up to 12 bursts allocated to the mobile starting with the CM service request. The TDOA data will be cached by the SCS.

The AMS will then capture and store in the call record, all messages from that mobile until it receives the setup message. Once the setup message is received, all information is available to determine if a location should be performed. The full origination, along with the mobile transmitted bits for the first 12 bursts are sent to the TLP. Missing frames will be indicated, and fill frames should be assumed.

With the complete origination information, the TLP will determine if a position determination is required. If so, the TLP will send a TOA\FOA request to the primary SCS. The request is similar to a TDOA request, but will also provide the uncoded data
5 bits. The primary SCS will then reply with the TOA, FOA, frequency offset, and phase corrections (if required) for each burst. The SCS will also provide SNR metrics for each burst.

The TLP will then send a TOA/FOA request to each of the SCSs, with the corrections
10 from the primary channel. The SCSs will process the data, and reply to the TLP with TOA, and FOA. The TLP will then execute the solve algorithm, and the position is determined.

The NIS will request the IMSI and MSISDN from the VLR, when needed. The NIS will
15 support the protocol stack for communication over the SS7 network, which allows communication with GSM VLRs, HLRs and MSCs.

Once the location is determined, the AP has the subscriber's information, and current location. If the subscriber has location service, the AP would send the location
20 information to the NIS, along with the IMSI, MSISDN, and routing information to the subscriber's current MSC. The NIS would then forward the location information to the subscriber in the form of a short message.

The location service could be a supplementary service defined in the subscriber's
25 information or kept in the AP database.

4.1 SCS Modifications

The SCS is not required to demodulate and identify all origination messages from the mobile phones. This will be accomplished by monitoring the Abis interface. For
30 station based processing, the SCS may have to demodulate only the bursts used for location, if those bits cannot be completely determined from the Abis interface, in cases of voice tracking.

- The SCS would, upon the receipt of a RACH Demod Request message from the TLP, search and demodulate a Random Access (RACH) Burst. The RACH Demod Request will contain the ARFCN, a time window to search, and the contents of the RACH
- 5 message to be demodulated. Upon successful demodulation and decoding of the RACH burst, the SCS may provide a RACH Demod Response message, with a time stamp to the TLP, indicating when the RACH burst occurred. If the RACH burst cannot be found, the SCS may provide an error message to the TLP, indicating that the RACH was not found.
- 10 The SCS could provide 200 kHz complex video bandwidth for TDOA data. The SCS could also provide the demodulated bits for a series of bursts upon request by the TLP, and may also provide frequency and phase corrections for each of these bursts (if necessary for accuracy). This could be sent to the other SCSs to be used for station based processing. The SCS could also provide a periodic message to the TLP, bound for the
- 15 AMS, which indicates the time drift between GPS and the T1 frame clock.

- Frame timing to the accuracy of a few microseconds can be initially determined by a search of a short burst (maybe a RACH burst) for each site in the system. This timing can then be maintained by counting the T1 frames in one of the SCSs, and calculating
- 20 Tdrift. Also, the TOA could be used to update the timing with each location. Upon receipt of a call cancel message, the SCS could match the hash code with the TDOA data stored in cache, and delete that TDOA data.

4.2 TLP Modifications

- 25 The TLP could be made to accept originations from the AMS, instead of the SCSs. The origination could be sent to the TLP in 2 messages, which can be linked by a hash code. The first message is just an indication that an origination has begun, and will include a timestamp. This message allows the TLP to start the TDOA data caching process. This caching process is probably not needed, as the phone does not reduce power for several
- 30 seconds. Data can be collected once an SOI is determined, from information in the seconds message. The second message will contain all information necessary for an origination (MIN, Dialed Digits).

The TLP could also provide a link in which the AMS can request a particular SCS to demodulate a RACH burst, and provide a timestamp back to the AMS. The TLP could accept RACH Demod Request Messages from the AMS and forward them to the
5 appropriate SCS. The TLP could also Accept RACH demod response messages from the SCS and forward them to the appropriate AMS. This allows the location system to know the relative timing of each Base Stations frame epoch.

Upon receipt of a call cancel message from the AMS, the TLP would link that call cancel
10 message to the origination message, and send a call cancel message to the appropriate SCSs. The TLP will then delete the origination form its memory.

4.3 Changes to the AP

The AP could be made to have an interface to the NIS, for the purpose of sending
15 short location related messages to mobile subscribers. The functionality of the NIS could be added to the AP, making the AP to NIS an internal interface.

4.4 Abis Monitoring System (AMS)

4.4.1 Call Tracking

20 The AMS may have a connection to the Abis interface of a BSC in the GSM system. This connection may provide the AMS bi-directional monitoring access to the Abis interface for each BTS under control of the BSC. The AMS may monitor the LAPD signaling link for the beacon TRX, for each cell, to allow location upon origination of calls. The AMS architecture may expand to monitor the LAPD signaling links for each
25 TRX, for all cells controlled by the BTS, to allow location using traffic channels. The AMS architecture may allow expansion to support up to 2000 LAPD signaling links. The AMS may detect call originations through the Immediate Assign Command. The AMS may identify emergency calls from the Immediate Assign Command.

30 Upon receipt of an Immediate Assign command, the AMS may notify the appropriate TLP within 25 milliseconds. The AMS may provide to the TLP with an origination indication, including a description of the physical channel assignment, a timestamp, and

a hash code to link with the origination information later. This hash code may also permit the TLP to request current physical channel information about a particular call, after voice channel assignment. (The same hash code is used throughout the duration of the call.) This process could wait for systems in which power control does not take effect
5 for several seconds (Ericsson Omnipoint), and a single origination message could be sent to the TLP.

The AMS may detect CM Service Request, Page Response, and Location Update Request, and link them to the Immediate Assign Command for a given call setup.
10

The AMS may detect Setup messages and Link them to the Immediate Assign Command for a given call setup.

If an Immediate Assign Command for a particular physical channel is sent to the BTS
15 before all of the origination information is gathered for the previous call, the AMS may send a call cancel message to the TLP, including the same hash code used for the origination indication message.

When the AMS has the complete origination information, consisting of the physical
20 channel, Mobile identity, and dialed digits, the AMS may forward this origination information to the TLP along with the same hash code used for the origination indication.

The AMS may detect Assignment Commands and Assignment Complete responses sent
25 over Abis interface for a given call, and link them to the original Immediate Assign Message.

The AMS may detect subsequent Hand-over Commands and Hand-over Failures to maintain the most up to date physical channel assignment for a given call. (Assignment
30 commands).

The AMS may accept Physical Channel request from the TLP. The TLP will provide the unique hash code which the AMS provided with the origination. The AMS may respond with a complete description of the Physical channel currently assigned to the call, or an indication that the AMS does not have the information. This will permit voice tracking,
5 which is initiated by the TLP.

The AMS may support inter AMS communication allowing inter BSC/MSC hand-over of call records. The Hand-over Command on the Abis interface provides the new cell ID, and hence the new AMS ID. Upon successful hand-over, the AMS will append the new
10 physical channel information to the call record, and send the entire call record to the new AMS, if the call is to be serviced by a different AMS.

The AMS may support up to 160 call arrivals per second.

15 4.3.2 TRX Configuration Maintenance

The AMS may have provided to it the configuration of each TRX controlled by the BSC. The configuration is defined as the TSC, a bit to indicate if frequency hopping is applied, the MAIO and HSN if frequency hopping is applied, or the ARFCN if frequency hopping is not applied. The AMS may maintain knowledge of the TRX
20 configuration by the following algorithm:

For each Assignment Command, or Immediate Assignment command, compare the Channel Description IE to the Channel Number IE of the n most recent successful Channel Activation Commands. Successful Channel Activation Commands are defined
25 as those with a Channel Activation Ack from the BTS. If the Channel Number IE of the Channel Activation matches the matches the Channel type and TDMA offset field, and the TN field of the Channel Description IE of the Assignment or Immediate Assignment Command of any of the n Channel Activation messages, store the TSC, H, MAIO and HSN, and ARFCN fields of the Channel Description IE. The AMS should maintain a list
30 of the fields from the last m Channel Description IEs, for each TRX. When any new Channel Description IE fields are added to the list, the new TRX configuration is defined as the configuration appearing most in the list of length m. If there is a tie, then the TRX

configuration may not be updated. If there are less than m sets of configuration values, the configuration may not be updated.

The parameter n may be an operator configurable parameter with a range of 1 to 12, a step size of 1, and a default value of 2. The parameter m may be an operator configurable parameter with a range of 1 to 12, a step size of 1, and a default value of 5.

The TRX configuration should be static, and any changes in TRX configuration should be known by the location system operator some time before the change takes place.

10 However, if the operator is not informed, the AMS will typically learn the new configuration after $m/2+1$ calls using that TRX.

4.3.3 Synchronization Maintenance

Upon initialization the AMS may monitor the signaling links on the Abis interface [AMS] for a Channel Required message for each cell controlled by the BSC. 15 Upon the receipt of the first Channel Required Message for a given cell, the AMS may store the frame number, F_0 , and time offset for the message, and request a timestamp determination from the TLP for that corresponding Channel Request message. In this request the AMS may include the ARFCN, a start time, and a search window length, the 20 Channel Request message contents, and a unique hash code. The search window length, W_1 may be an operator configurable parameter with a range of 1 to 500 milliseconds, with a step size of 1 millisecond, and a default value of 100 milliseconds. The TLP will forward this message to the appropriate SCS and eventually reply with a timestamp, and a signal quality measurement, if the burst is found, other wise, an indication that the 25 burst was not found. If the burst was not found, the AMS repeats the process with the next Channel Required message.

When the AMS finally receives a successful timestamp for the burst, it calculates the time of the Epoch of the stored frame as GPS timestamp – Access delay, T_0 . Any 30 subsequent frame epoch can be determined by:

$$T_{\text{frame}} = (F_1 - F_0) * 60/13 + T_0.$$

The epoch for any TNx in a frame can be determined by:

$$T_{\text{frame}} + x15/26 \text{ milliseconds.}$$

Upon successful determination of the frame epoch, the AMS may start a Timer, T501.

- 5 When the timer expires, the AMS may reinitiate the epoch capture procedure. T501 may be an operator configurable parameter with a range of 1 second to 36000 seconds with a one-second-step size, and a default value of 900 seconds.

- 10 A single SCS will be configured to provide a time drift measurement, Tdrift, between the GPS time and the T1 clock. This SCS will provide a drift offset once each L seconds. Each L seconds the Tframe may be adjusted by the Tdrift. L may be an operator configurable parameter with a range of 1 to 900 seconds, step size of 1 seconds and a default value of 10 seconds.

15 4.4 NIS

The NIS could be part of the AP, and therefore need not have an explicit interface to the AP.

4.4.1 Subscriber Identification

- 20 The NIS may connect to the all VLRs in a GSM network. The NIS may connect to up to 5 VLRs. The NIS may comply with GSM 09.02 for communication with the VLR. The VLR may have a link to each AMS in the network. The NIS may support link for up to 10 AMS in the network.
- 25 The NIS may accept subscriber information request messages from each AMS in the network. The subscriber request may contain the subscriber's TMSI, or IMSI, and the VLR number with which the subscriber is registered. Upon receiving the subscriber request message, the NIS may issue a send parameters command to the appropriate VLR, and request the subscriber information. Upon successful reception of the subscriber
- 30 information from the VLR, the NIS may forward it to the requesting AMS. If the request was unsuccessful, an error message may be forwarded to the requesting AMS.

4.4.2 Short Message Service

The NIS may provide an interface to the AP. This interface will allow the AP to send short messages to a subscriber, containing the subscriber's location, or any location related data. The NIS may accept SMS requests from the AP, and forward the short messages to the appropriate MSC. Upon successful delivery of the short message, the NIS may provide an acknowledgement to the AP. If the network was unsuccessful delivering the message, the NIS may inform the AP. The NIS may comply with GSM specification 09.02, when communicating with the Network.

10 Conclusion

The true scope the present invention is not limited to the presently preferred embodiments disclosed herein. For example, the foregoing disclosure of a presently preferred embodiment of a Wireless Location System uses explanatory terms, such as Signal Collection System (SCS), TDOA Location Processor (TLP), Applications Processor (AP), and the like, which should not be construed so as to limit the scope of protection of the following claims, or to otherwise imply that the inventive aspects of the system are limited to the particular methods and apparatus disclosed. Moreover, as will be understood by those skilled in the art, many of the inventive aspects disclosed herein may be applied in location systems that are not based on TDOA techniques. For example, the processes by which the Wireless Location System determines TDOA and FDOA values can be applied to non-TDOA systems. Similarly, the invention is not limited to systems employing SCS's constructed as described above, nor to systems employing AP's meeting all of the particulars described above. The SCS's, TLP's and AP's are, in essence, programmable data collection and processing devices that could take a variety of forms without departing from the inventive concepts disclosed herein. Given the rapidly declining cost of digital signal processing and other processing functions, it is easily possible, for example, to transfer the processing for a particular function from one of the functional elements (such as the TLP) described herein to another functional element (such as the SCS or AP) without changing the inventive operation of the system. In many cases, the place of implementation (i.e., the functional element) described herein is merely a designer's preference and not a hard requirement. Accordingly, except as they may be expressly so limited, the scope of protection of the

following claims is not intended to be limited to the specific embodiments described above.

CLAIMS

What is claimed is:

1. A mobile station (MS) management method for a wireless location system
5 (WLS) that estimates the geographic location of said mobile transmitter, wherein the WLS overlays at least a portion of the geographic area of a wireless communications system, wherein the WLS includes radio resources and location processing resources, and wherein the wireless communications system includes base transceiver station (BTS) equipment connected to base station controller (BSC) equipment, comprising the steps
10 of:
 - continuously monitoring the communications between at least one BTS and at least one BSC,
 - extracting MS information from the monitored communications, and
 - forwarding the extracted MS information to the WLS.
- 15 2. A method as recited in claim 1, wherein the extracted MS information may include the mobile station identification (MSID), the called number dialed by the user of the MS, the contents of messages sent to the MS or from the MS, or frequency assignment information sent to the MS.
- 20 3. A method as recited in claim 1, wherein the extracted MS information may include any of the following presently in use by the MS: the control channel, the traffic channel, the mobile directory number (MDN), the Electronic Serial Number (ESN), the Mobile Identity Number (MIN), the Mobile Subscriber Identification (MSI), the
25 international mobile subscriber identity (IMSI), the temporary mobile subscriber identity (IMSI), or the mobile station international ISDN number (MSISDN).
4. A method as recited in claim 1, wherein the WLS uses the extracted MS information to determine whether to perform location processing for said MS.

30

5. A method as recited in claim 1, wherein the WLS uses the extracted MS information to determine which radio resources to use in performing location processing for said MS.

5 6. A method as recited in claim 1, wherein the WLS uses the extracted MS information to determine which location processing resources to use in performing location processing for said MS.

7. A method as recited in claim 1, wherein the WLS stores the extracted MS
10 information in a database.

8. A method as recited in claim 7, wherein the WLS removes the extracted MS information from the database after the extracted MS information is no longer valid.

15 9. A method as recited in claim 8, wherein the extracted MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

10. A method as recited in claim 8, wherein the extracted MS information is
20 determined to be no longer valid because a predetermined period of time has expired.

11. A method as recited in claim 8, wherein the extracted MS information is determined to be no longer valid because a predetermined period of time has expired without an update to the extracted MS information.

25 12. A method as recited in claim 1, wherein the WLS discards the extracted MS information if the extracted MS information does not match any of a set of predetermined criteria.

30 13. A method as recited in claim 12, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

14. A method for use in a wireless location system (WLS), wherein the WLS overlays at least a portion of a wireless communications system that includes base transceiver station (BTS) equipment operatively coupled to base station controller (BSC) equipment via an interface, comprising the steps of:

5 monitoring communications on the interface between at least one BTS and at least one BSC;

 identifying certain prescribed mobile station (MS) information from the monitored communications;

10 forwarding the MS information to the WLS; and

 using the MS information to determine whether to perform location processing for said MS and/or to determine which radio resources to use in performing location processing for said MS and/or to determine which location processing resources to use in performing location processing for said MS.

15

15. A method as recited in claim 14, wherein the MS information includes one or more of the following: a mobile station identification (MSID), a called number, contents of messages sent to the MS or from the MS, and/or frequency assignment information sent to the MS.

20

16. A method as recited in claim 14, wherein the MS information includes one or more of the following presently in use by the MS: control channel, traffic channel, mobile directory number (MDN), Electronic Serial Number (ESN), Mobile Identity Number (MIN), Mobile Subscriber Identification (MSI), international mobile subscriber identity (IMSI), temporary mobile subscriber identity (TMSI), and/or mobile station international ISDN number (MSISDN).

25

17. A method as recited in claim 14, wherein the WLS stores the MS information in a database.

30

18. A method as recited in claim 17, wherein the WLS removes the MS information from the database after the MS information is no longer valid.

19. A method as recited in claim 18, wherein the MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

5

20. A method as recited in claim 18, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired.

21. A method as recited in claim 18, wherein the MS information is determined
10 to be no longer valid because a predetermined period of time has expired without an update to the MS information.

22. A method as recited in claim 14, wherein the WLS discards the MS
information if the MS information does not match any of a set of predetermined criteria.

15

23. A method as recited in claim 22, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

20 24. A wireless location system (WLS) that overlays at least a portion of a wireless communications system that includes base transceiver station (BTS) equipment operatively coupled to base station controller (BSC) equipment via an interface, comprising:

means for monitoring communications on the interface between at least one BTS
25 and at least one BSC;

means for identifying certain prescribed mobile station (MS) information from the monitored communications; and

means for using the MS information to determine whether to perform location processing for said MS and/or to determine which radio resources to use in performing
30 location processing for said MS and/or to determine which location processing resources to use in performing location processing for said MS.

25. A system as recited in claim 24, wherein the MS information includes one or more of the following: a mobile station identification (MSID), a called number, contents of messages sent to the MS or from the MS, and/or frequency assignment information sent to the MS.

5

26. A system as recited in claim 24, wherein the MS information includes one or more of the following presently in use by the MS: control channel, traffic channel, mobile directory number (MDN), Electronic Serial Number (ESN), Mobile Identity Number (MIN), Mobile Subscriber Identification (MSI), international mobile subscriber identity (IMSI), temporary mobile subscriber identity (TMSI), and/or mobile station international ISDN number (MSISDN).

10

27. A system as recited in claim 24, further comprising a database, wherein the WLS stores the MS information in said database.

15

28. A system as recited in claim 27, wherein the WLS removes the MS information from the database after the MS information is no longer valid.

29. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because the MS is no longer registered with the wireless communications system.

20

30. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired.

25

31. A system as recited in claim 28, wherein the MS information is determined to be no longer valid because a predetermined period of time has expired without an update to the MS information.

30

32. A system as recited in claim 24, wherein the WLS discards the MS information if the MS information does not match any of a set of predetermined criteria.

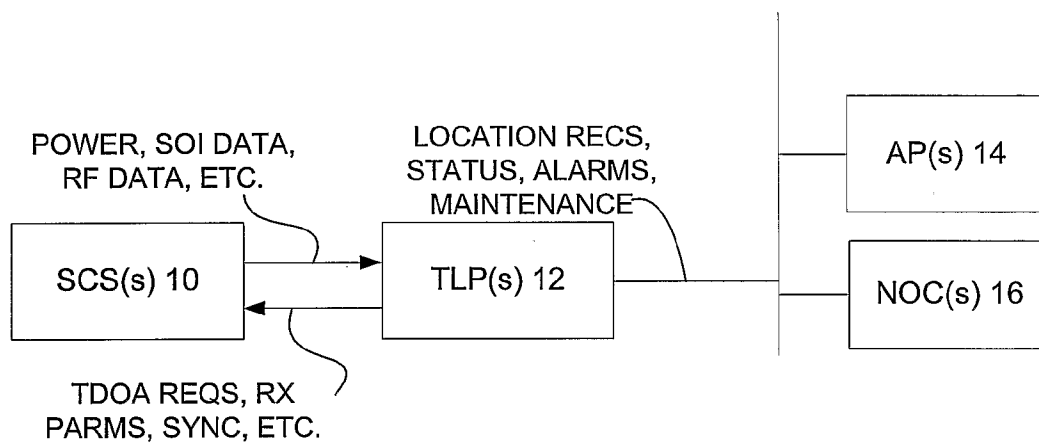
33. A system as recited in claim 32, wherein the set of predetermined criteria includes information about the identity of the MS or the number called by the user of the MS.

5

ABSTRACT OF THE DISCLOSURE

In an overlay Wireless Location System, an Abis interface is monitored to obtain information used to locate GSM phones. Signaling links of the Abis interface are passively monitored to obtain certain information, such as control and traffic channel
5 assignment, called number, and mobile identification, which is not available from the GSM air interface of the reverse channel. This approach also applies to IDEN and can be broadened to include CDMA systems where the GSM architecture has been used and the system includes a separated BTS to BSC interface.

1/31

**FIGURE 1**

2/31

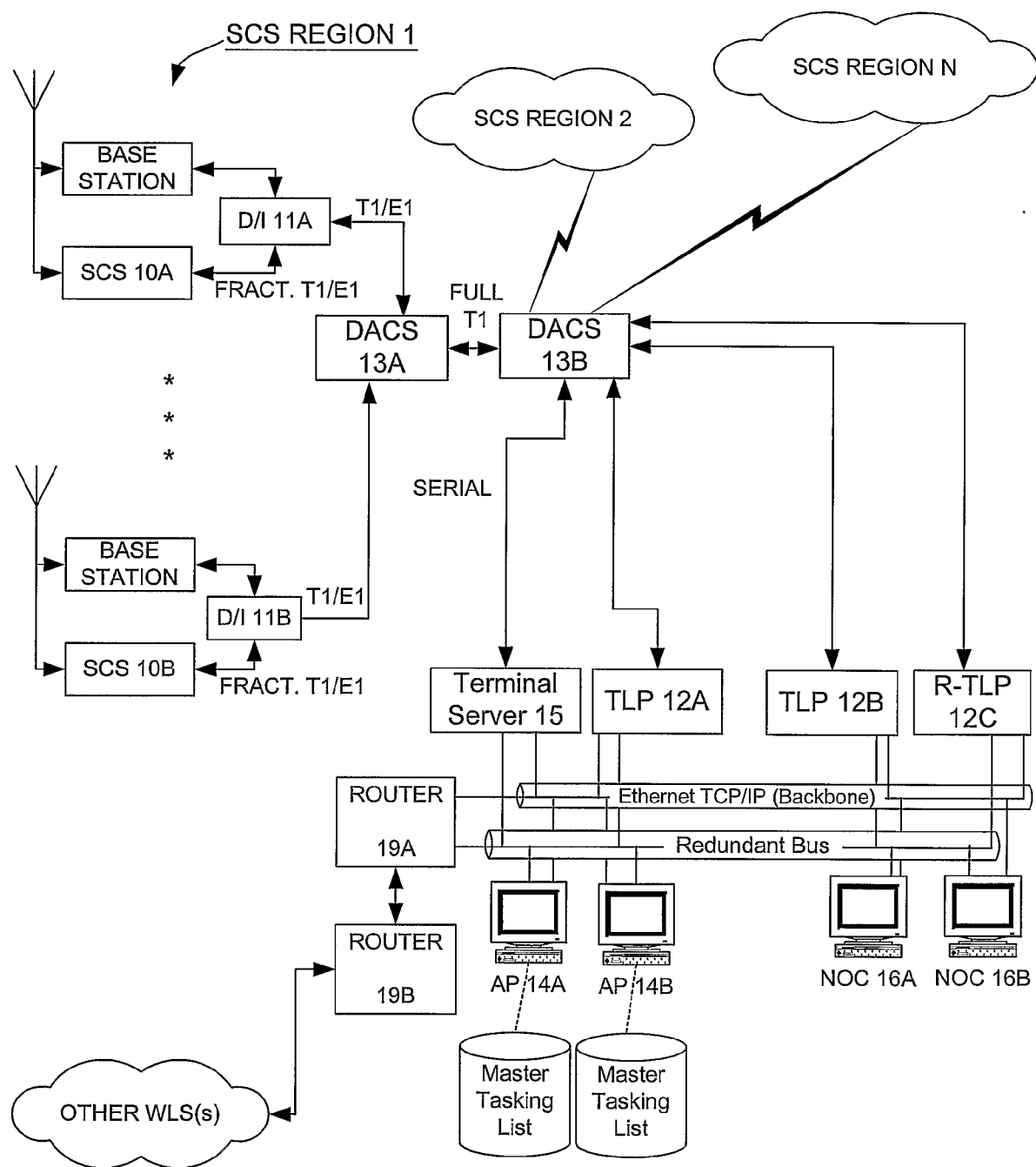


FIGURE 1A

3/31

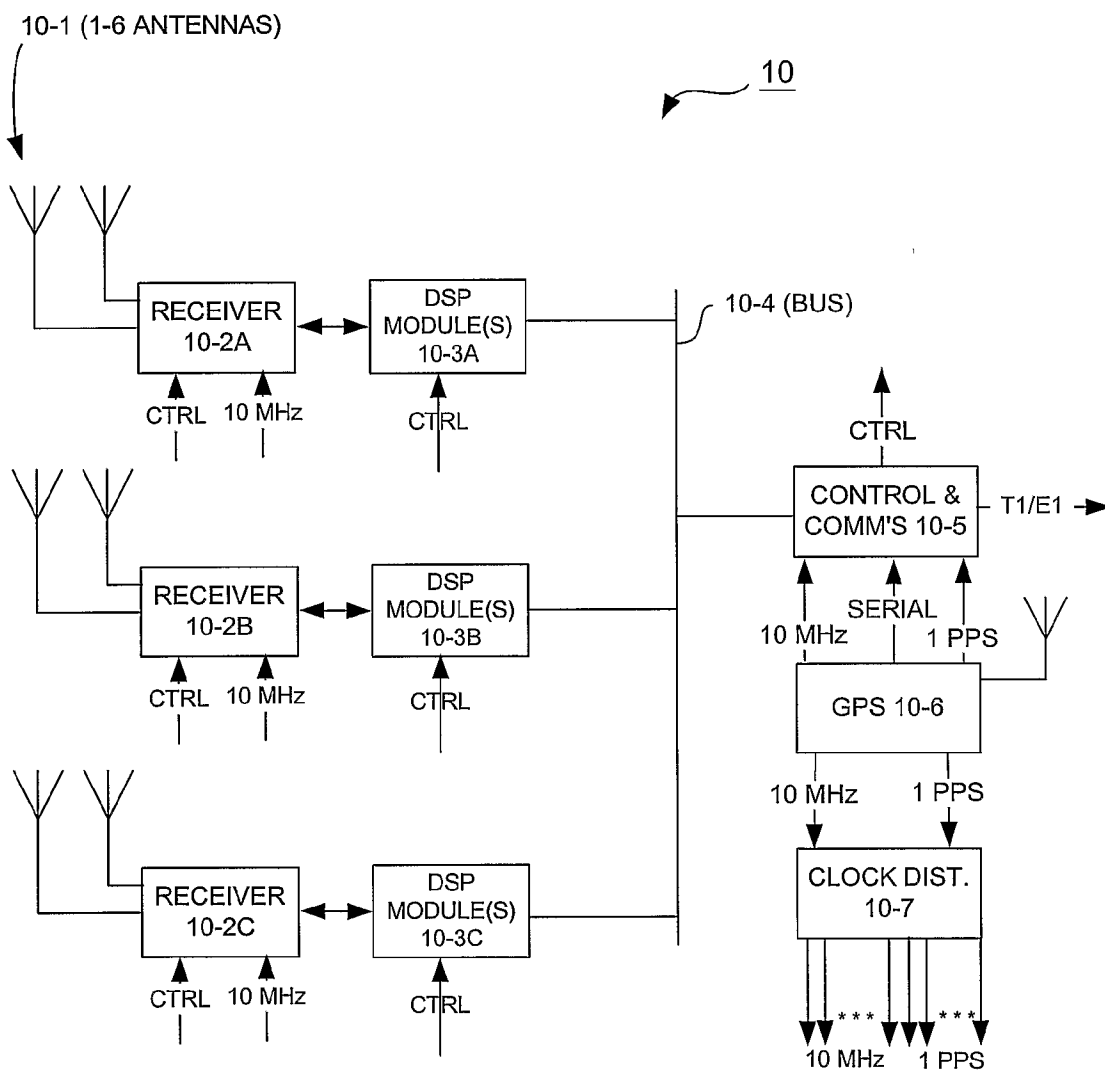


FIGURE 2

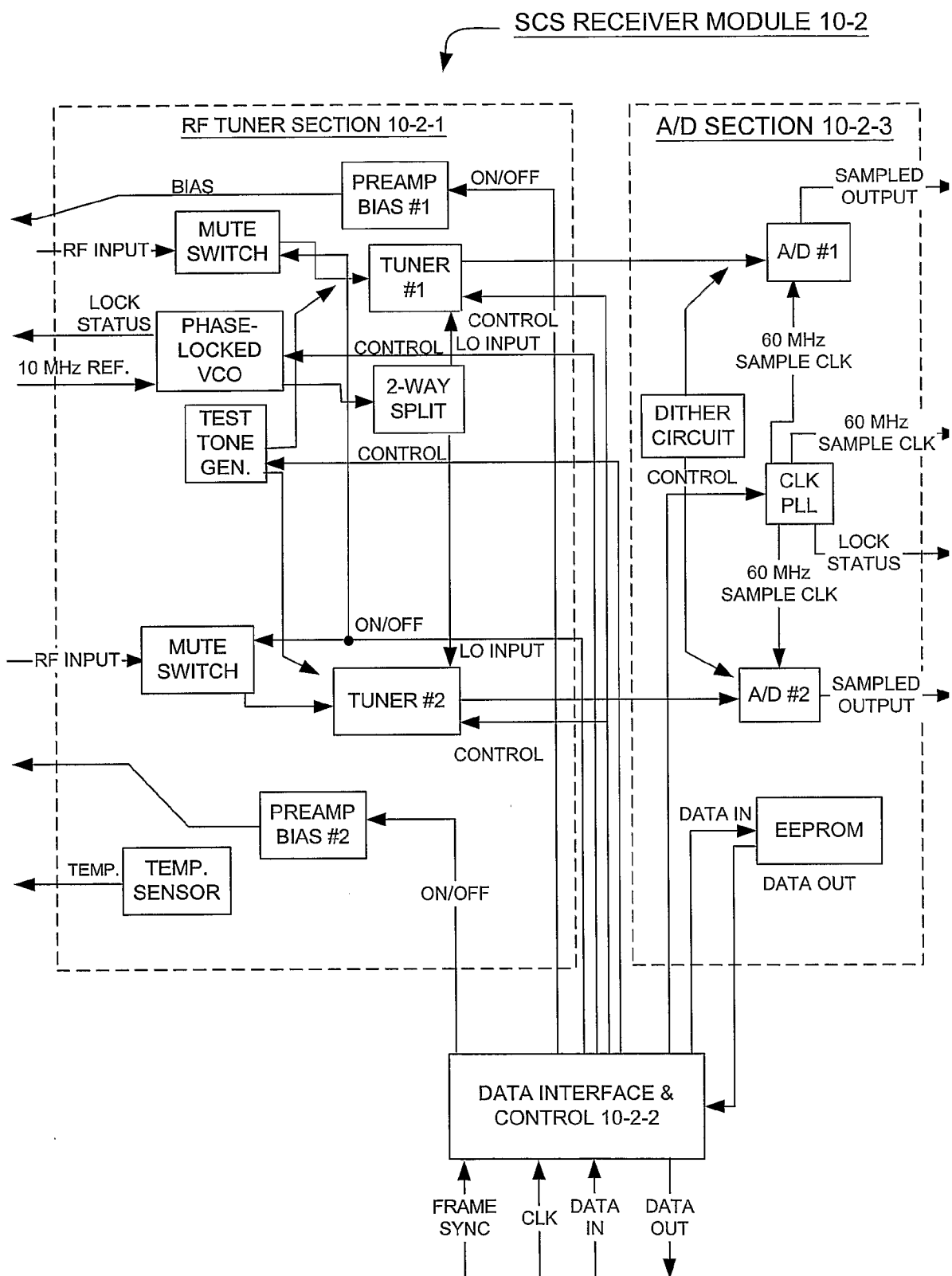
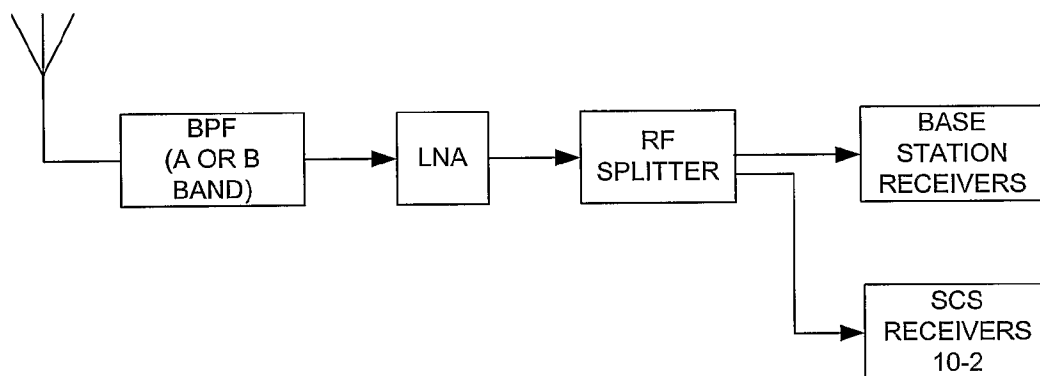
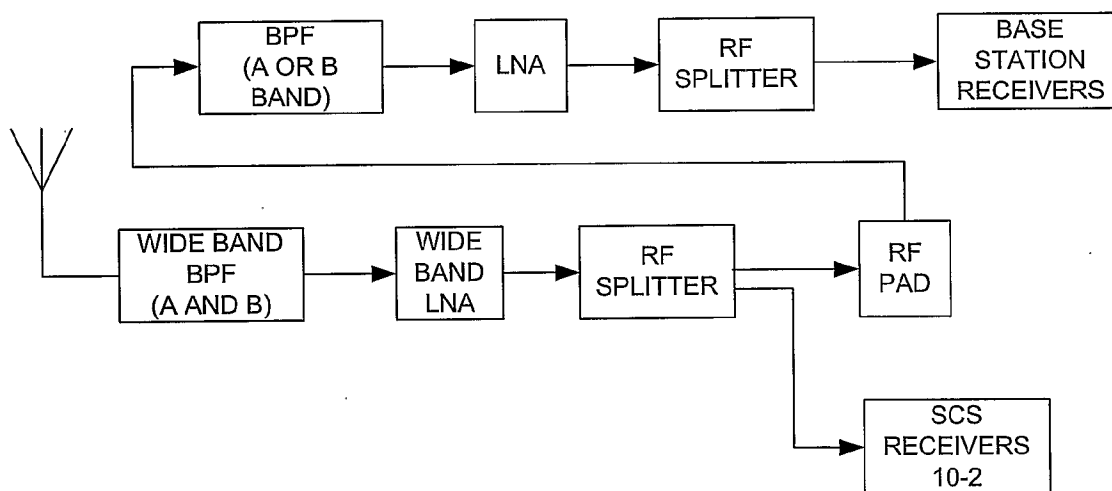


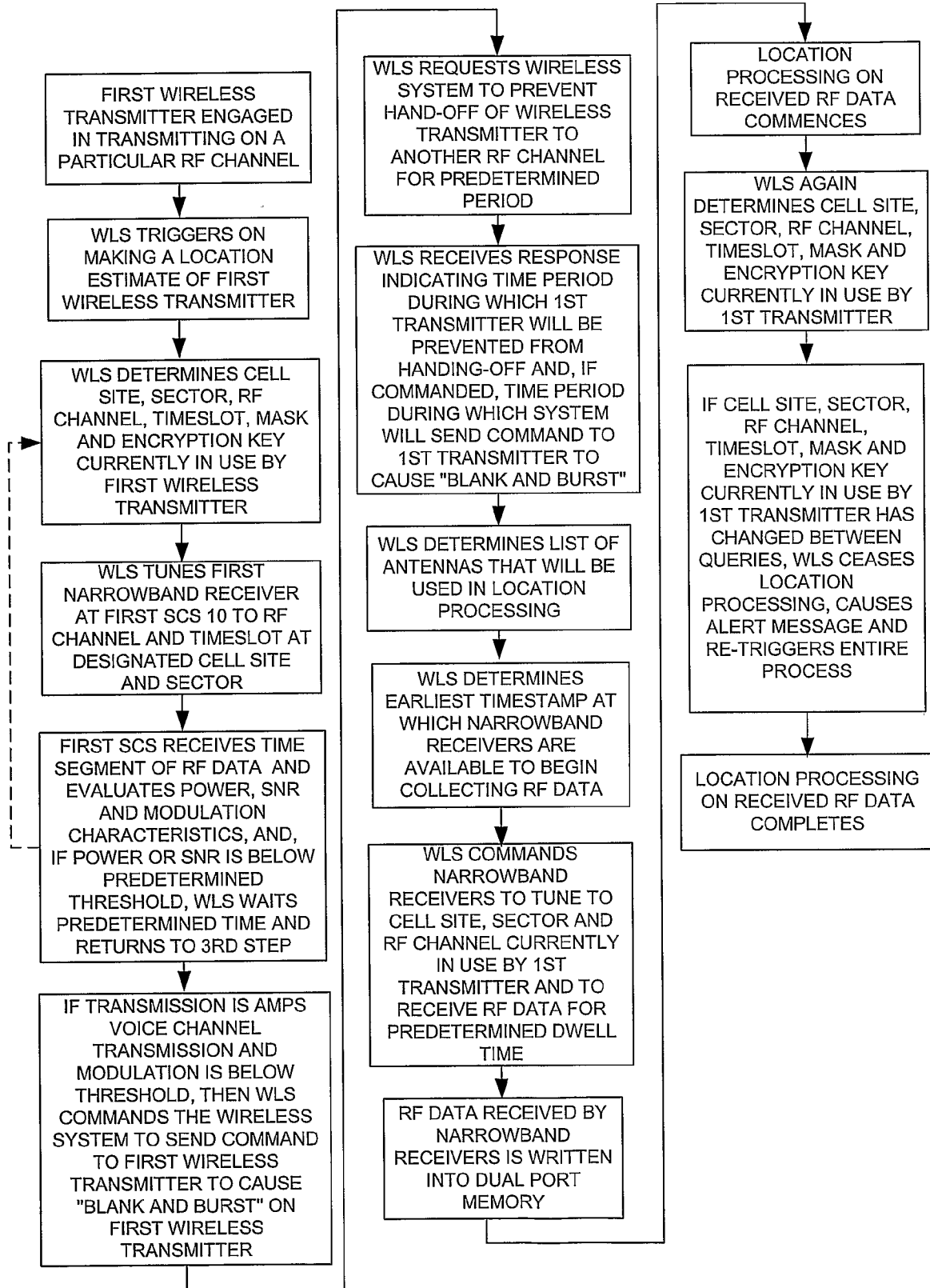
FIGURE 2A

SUBSTITUTE SHEET (RULE 26)

5/31

**FIGURE 2B****FIGURE 2C**

6/31



7/31

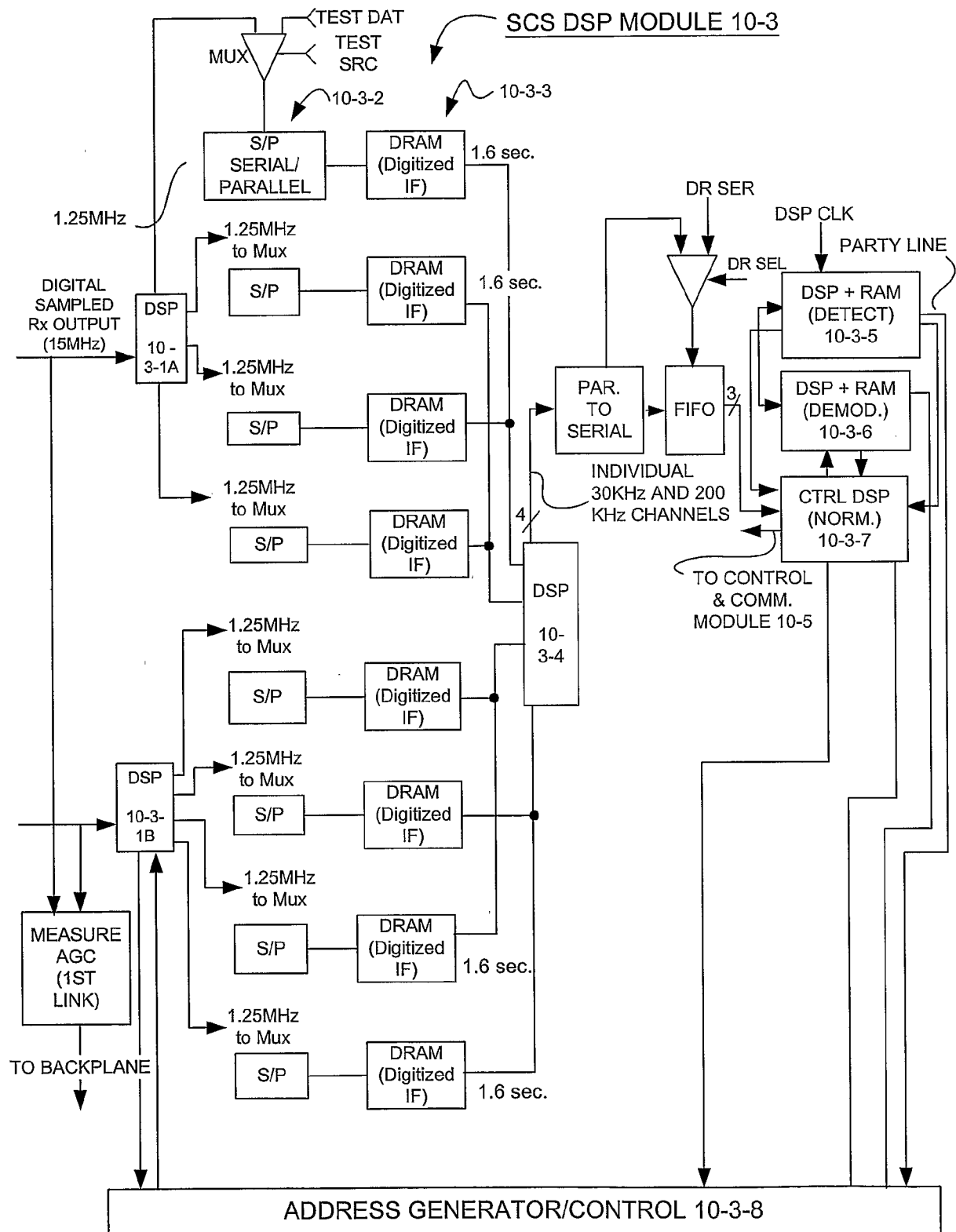
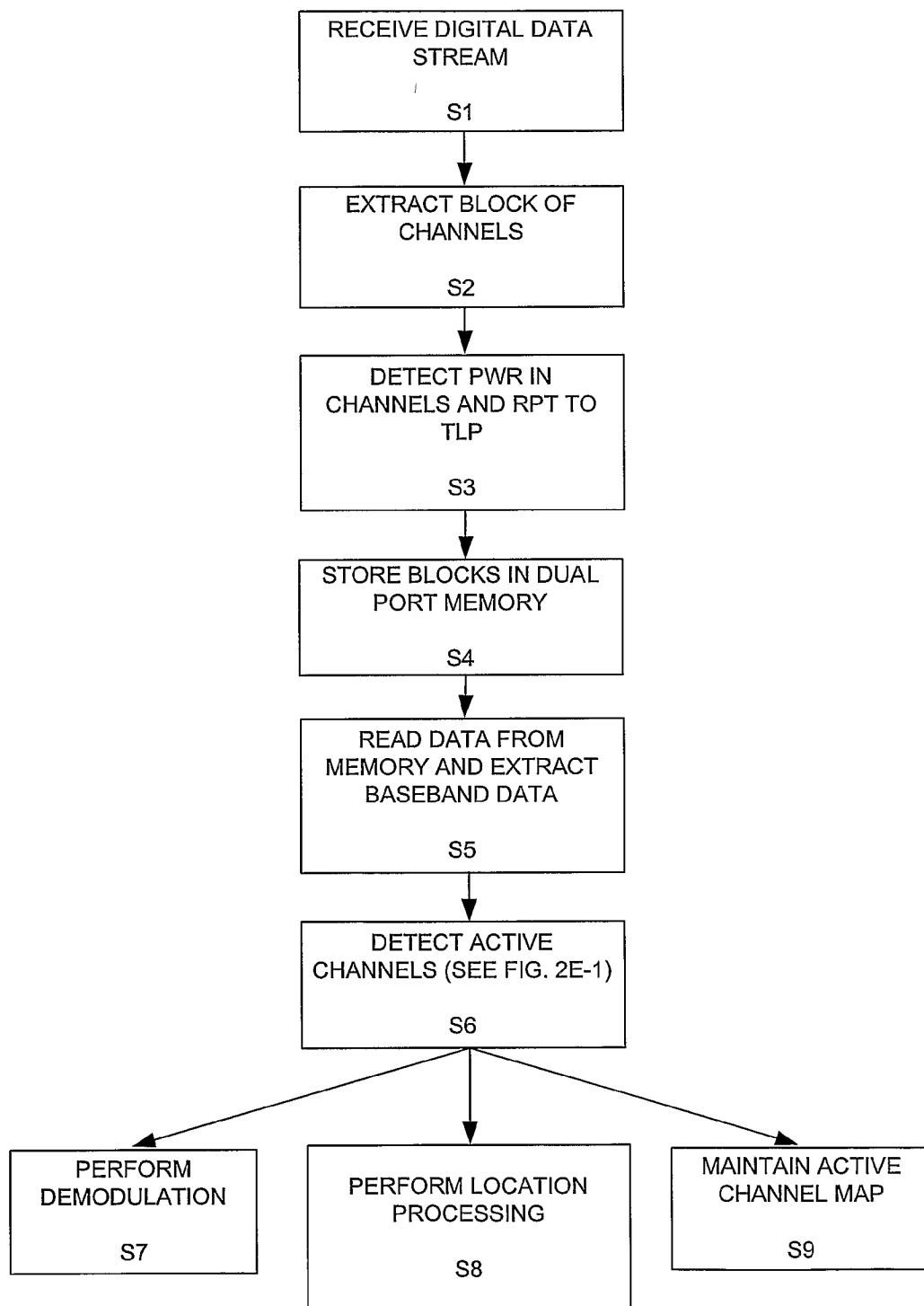


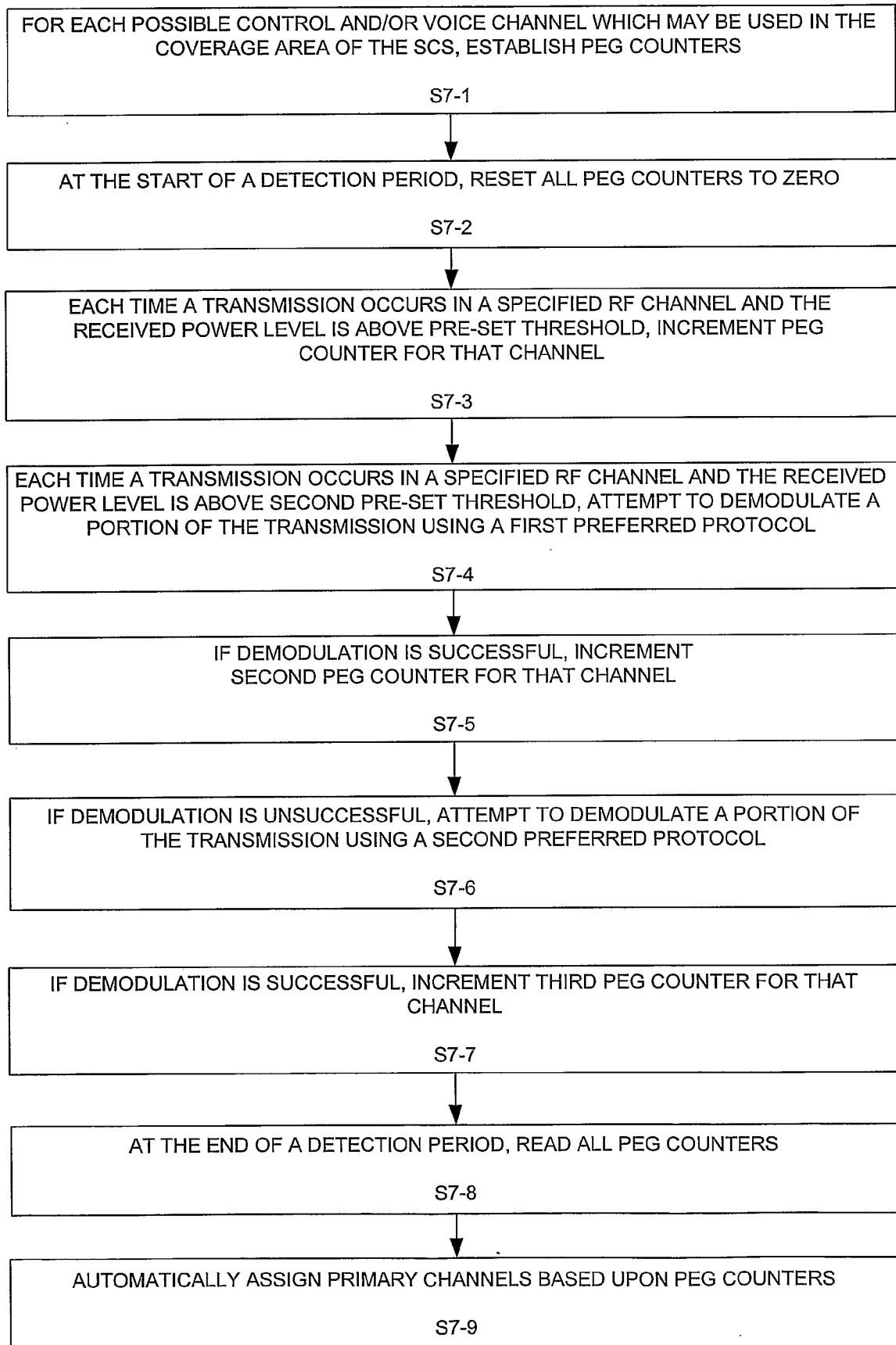
FIGURE 2D

SUBSTITUTE SHEET (RULE 26)

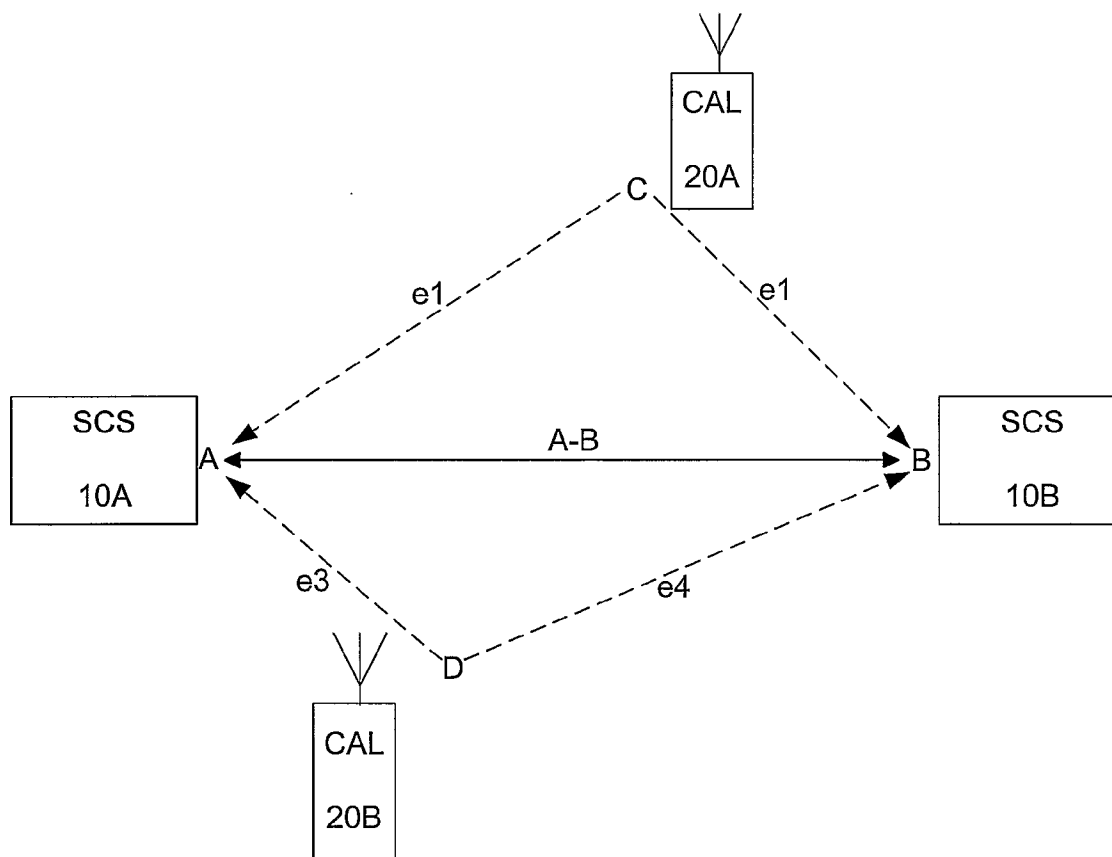
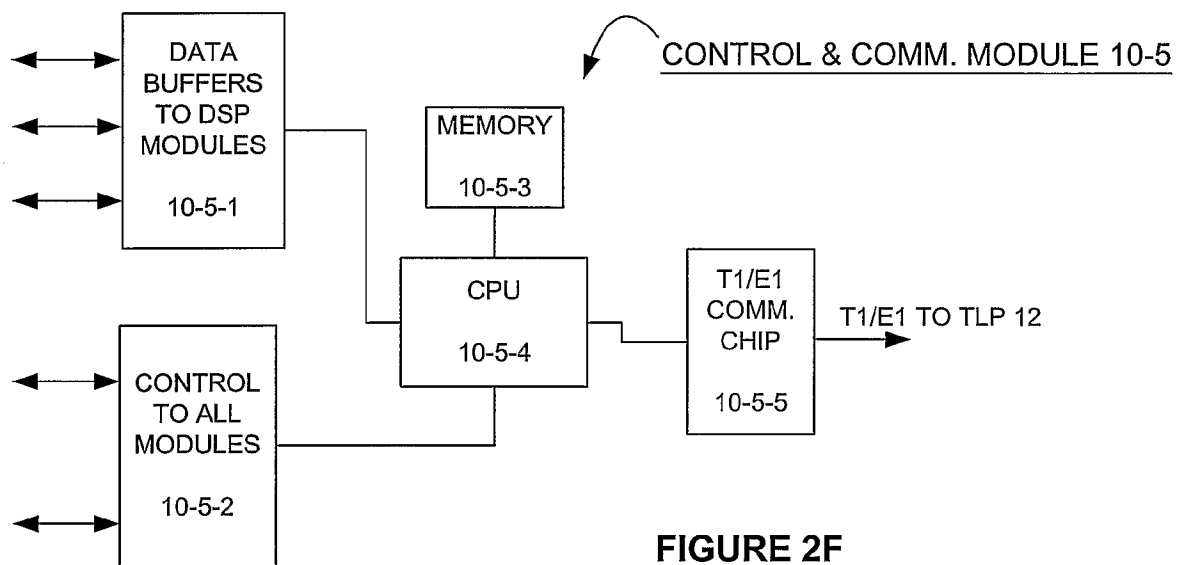
8/31

**FIGURE 2E**

9/31

**FIGURE 2E-1**

10/31



11/31

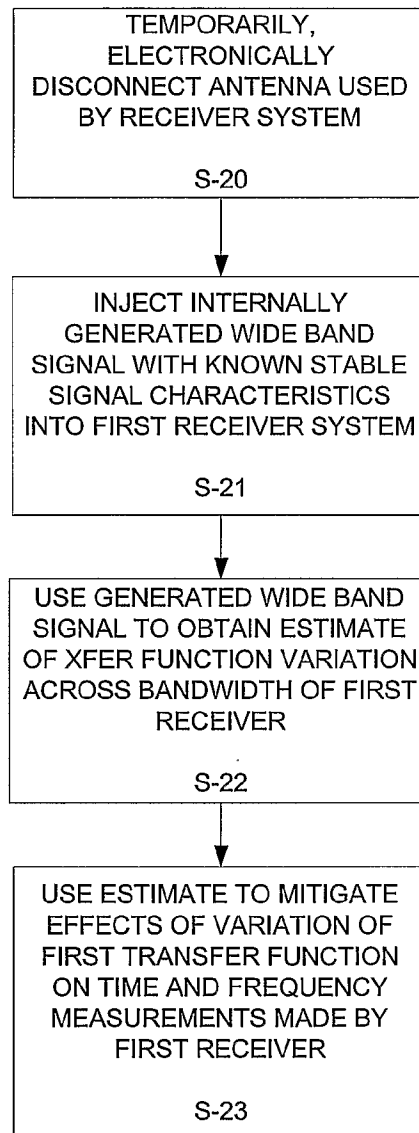


FIGURE 2H

12/31

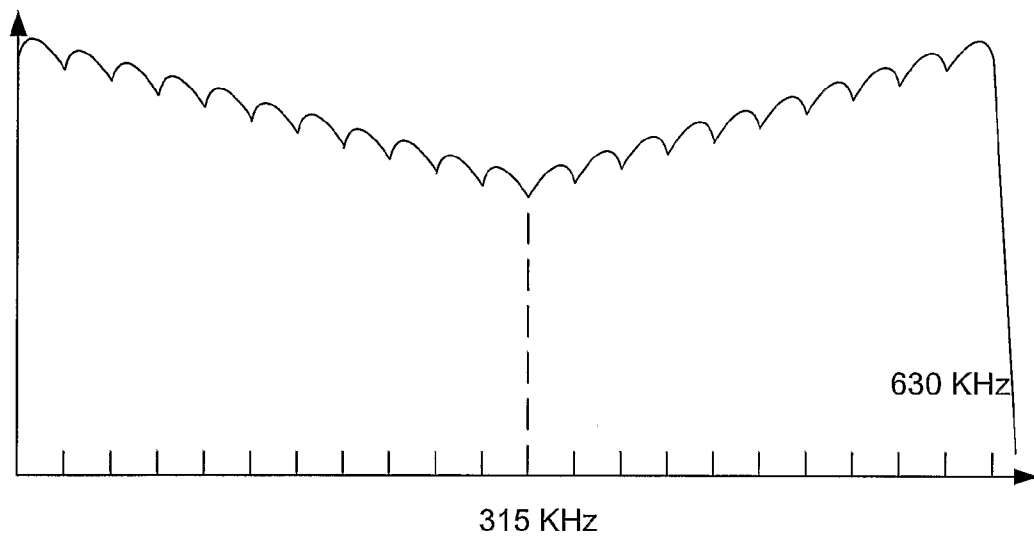


FIGURE 2I

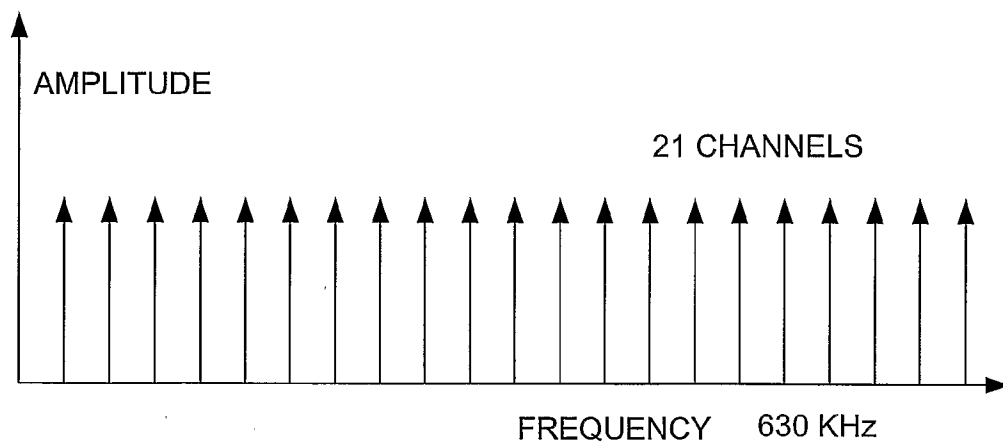


FIGURE 2J

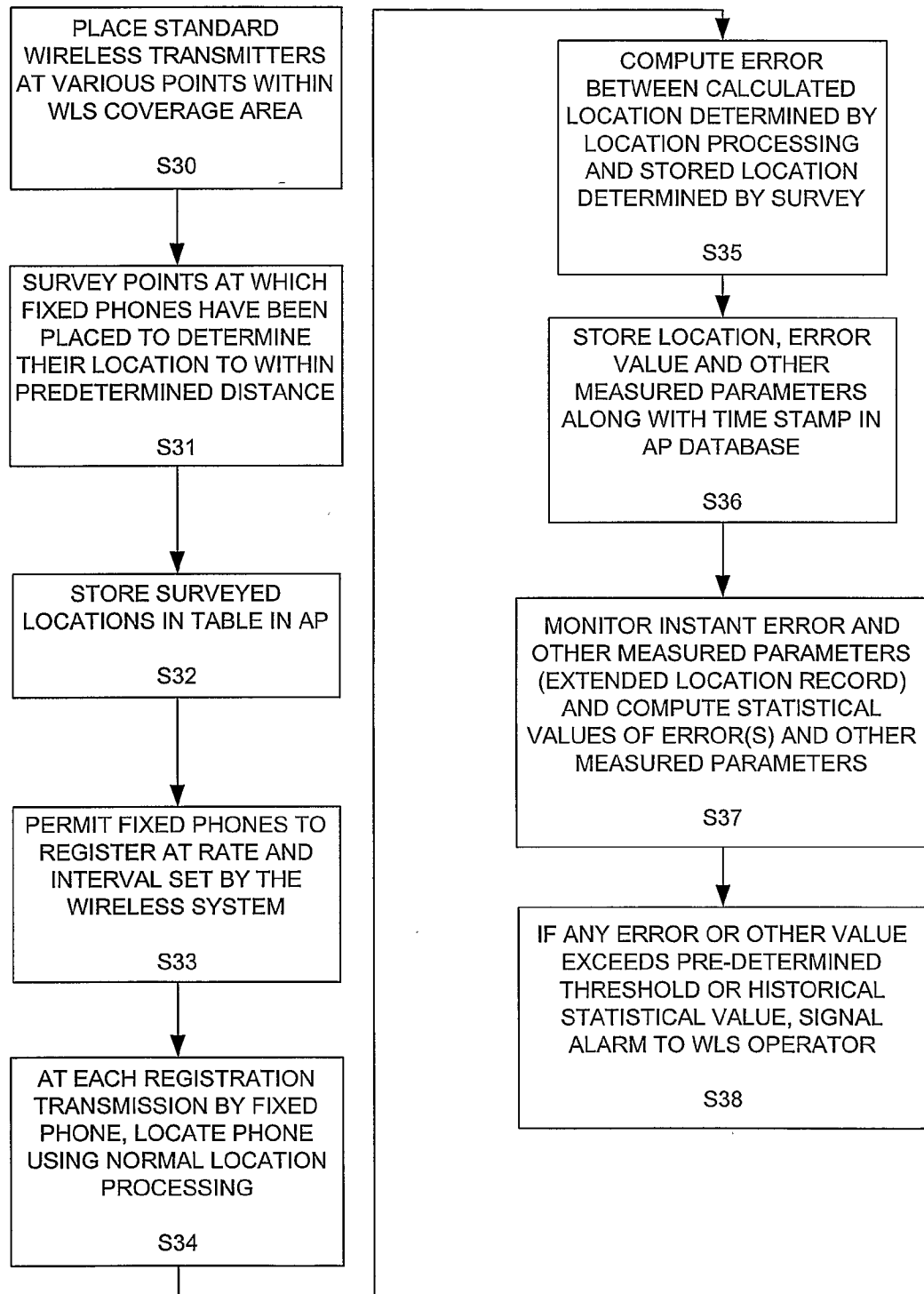


FIGURE 2K

14/31

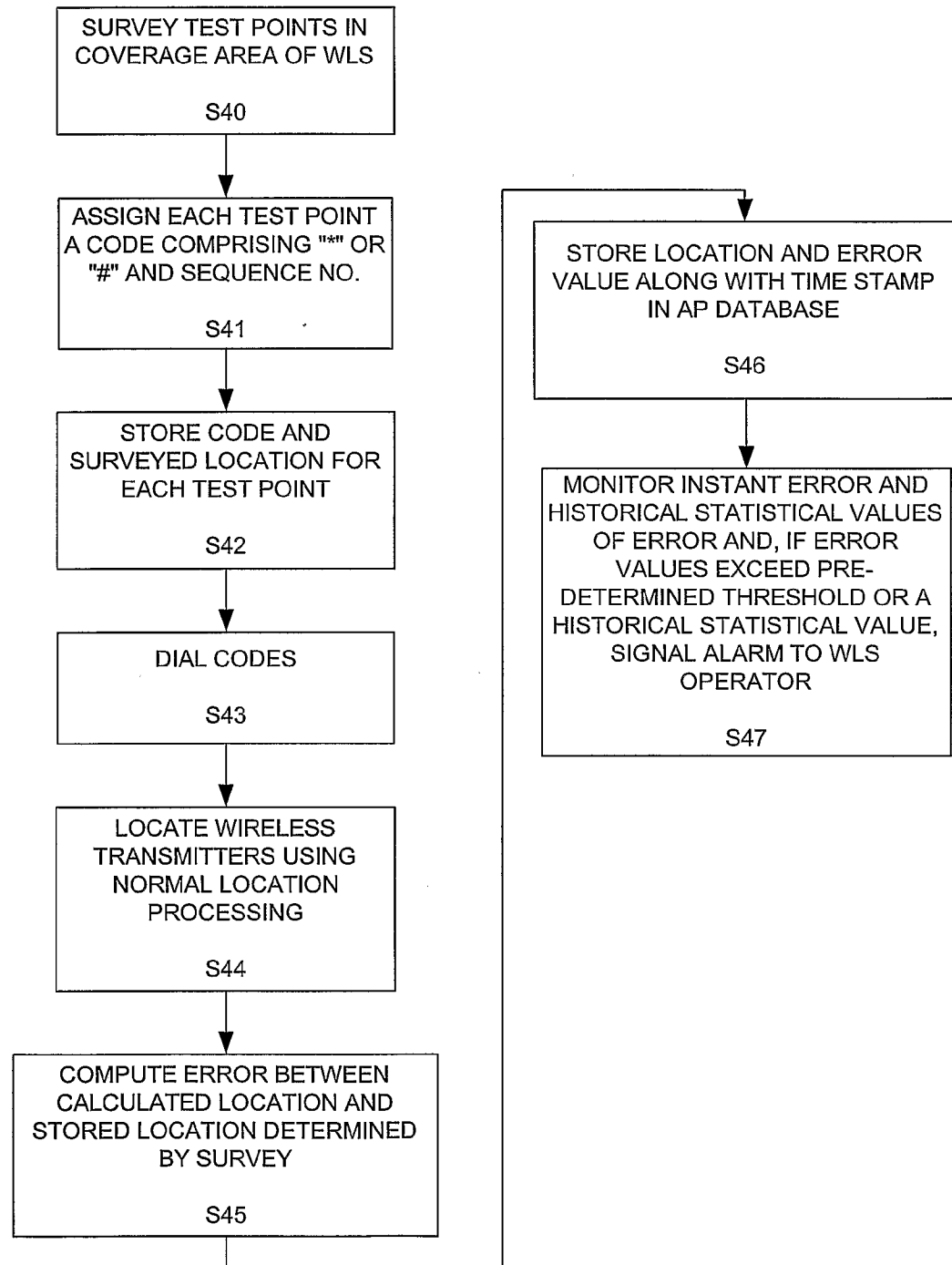


FIGURE 2L

SUBSTITUTE SHEET (RULE 26)

15/31

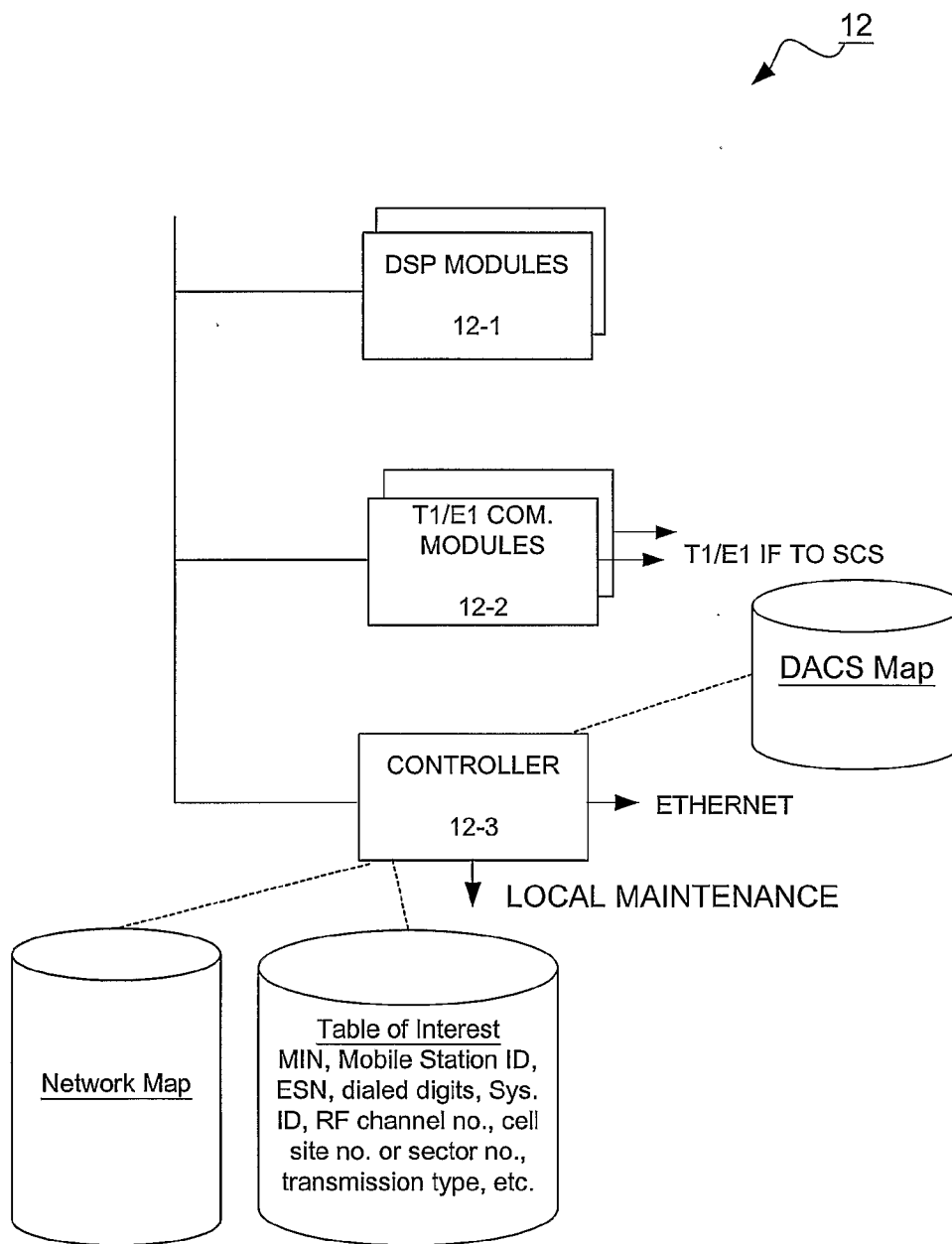


FIGURE 3

16/31

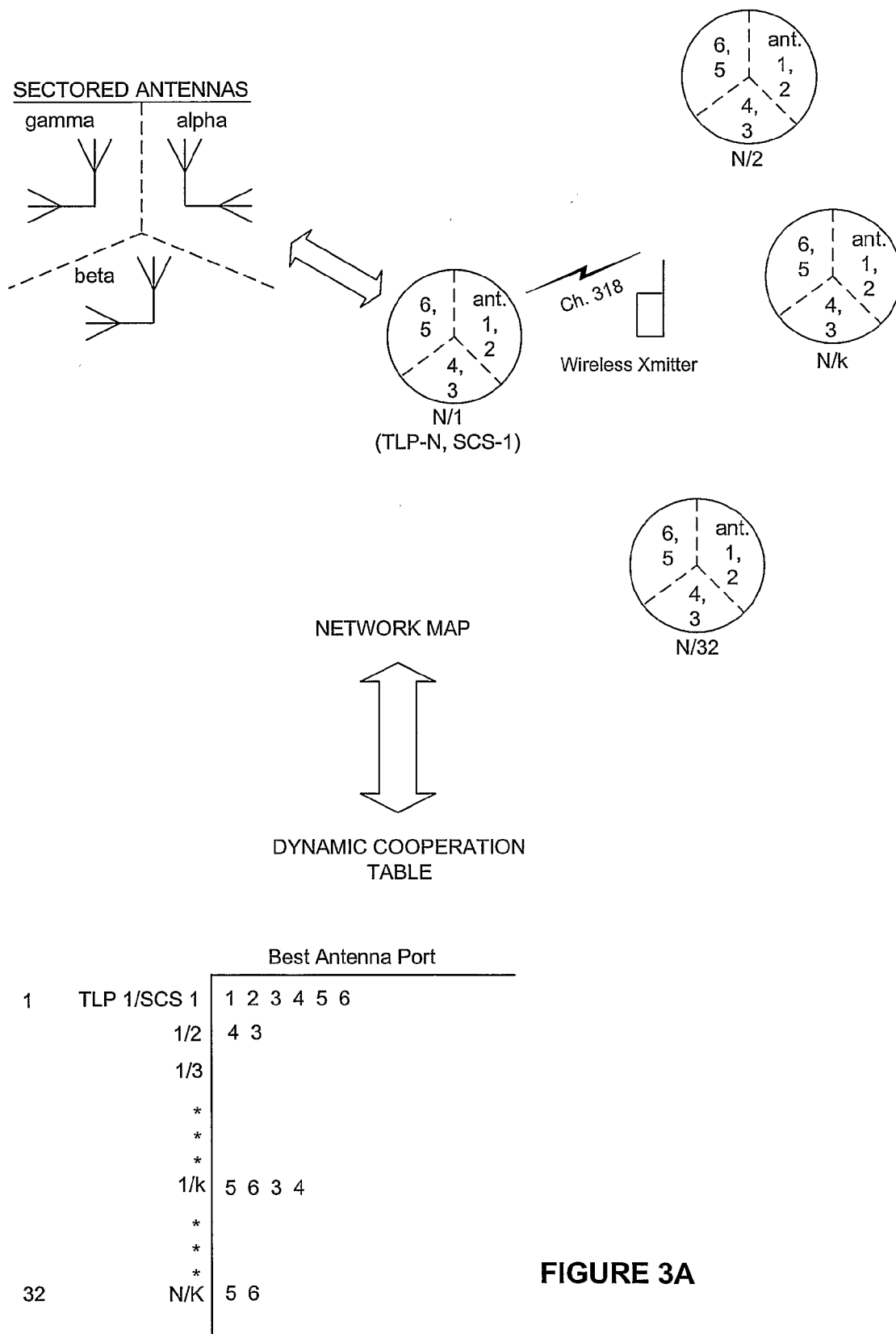


FIGURE 3A

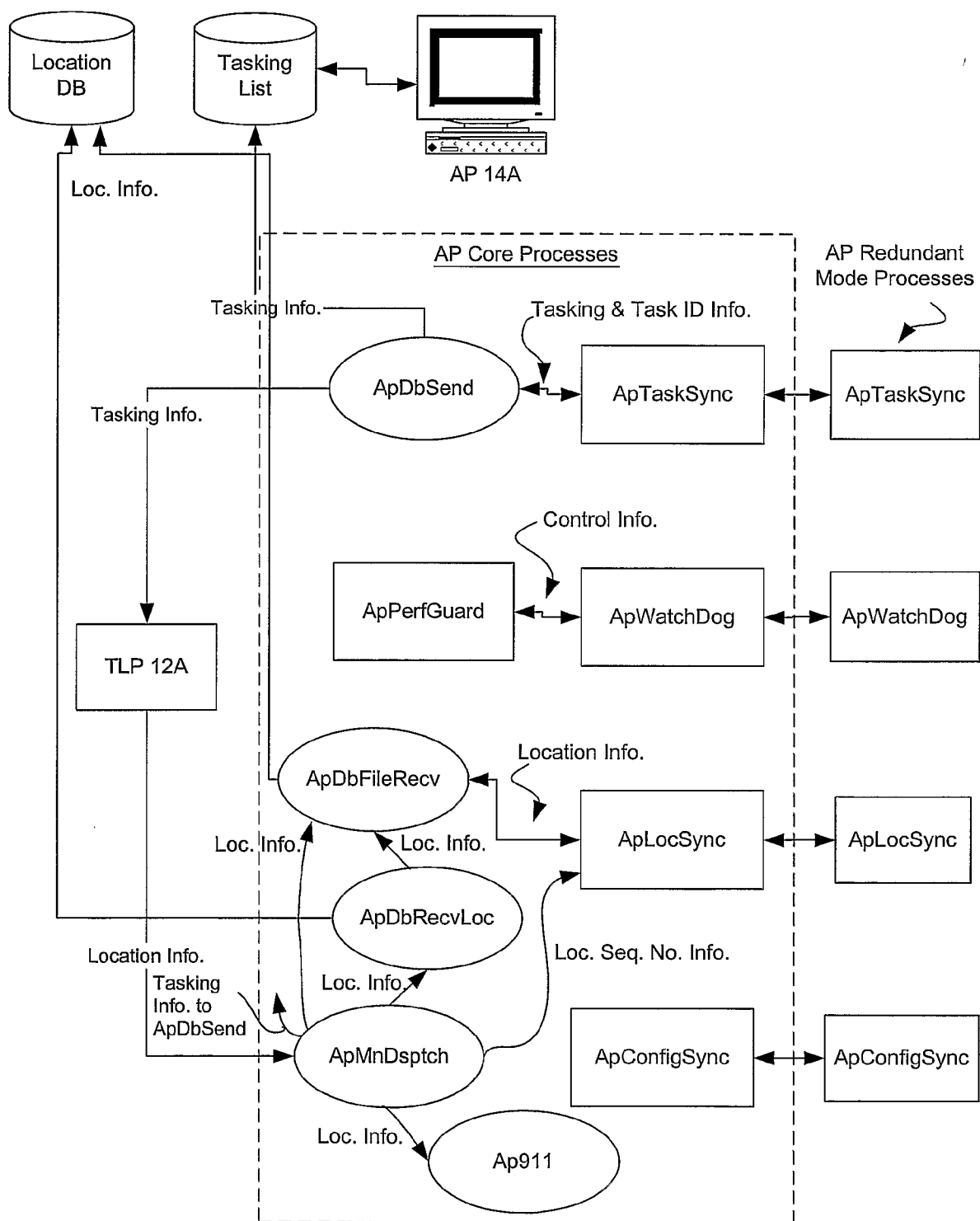
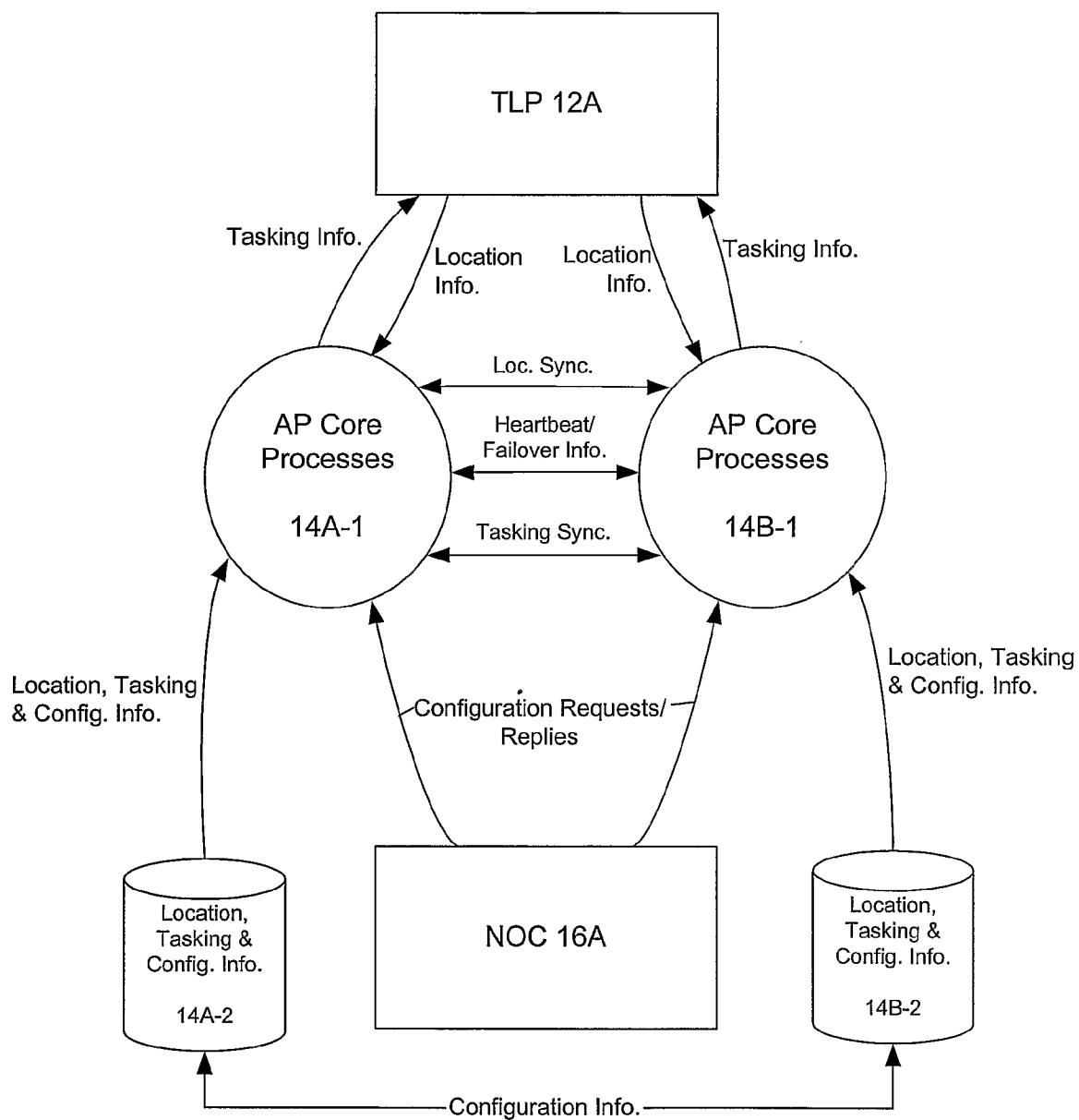


FIGURE 4

18/31

**FIGURE 4A**

19/31

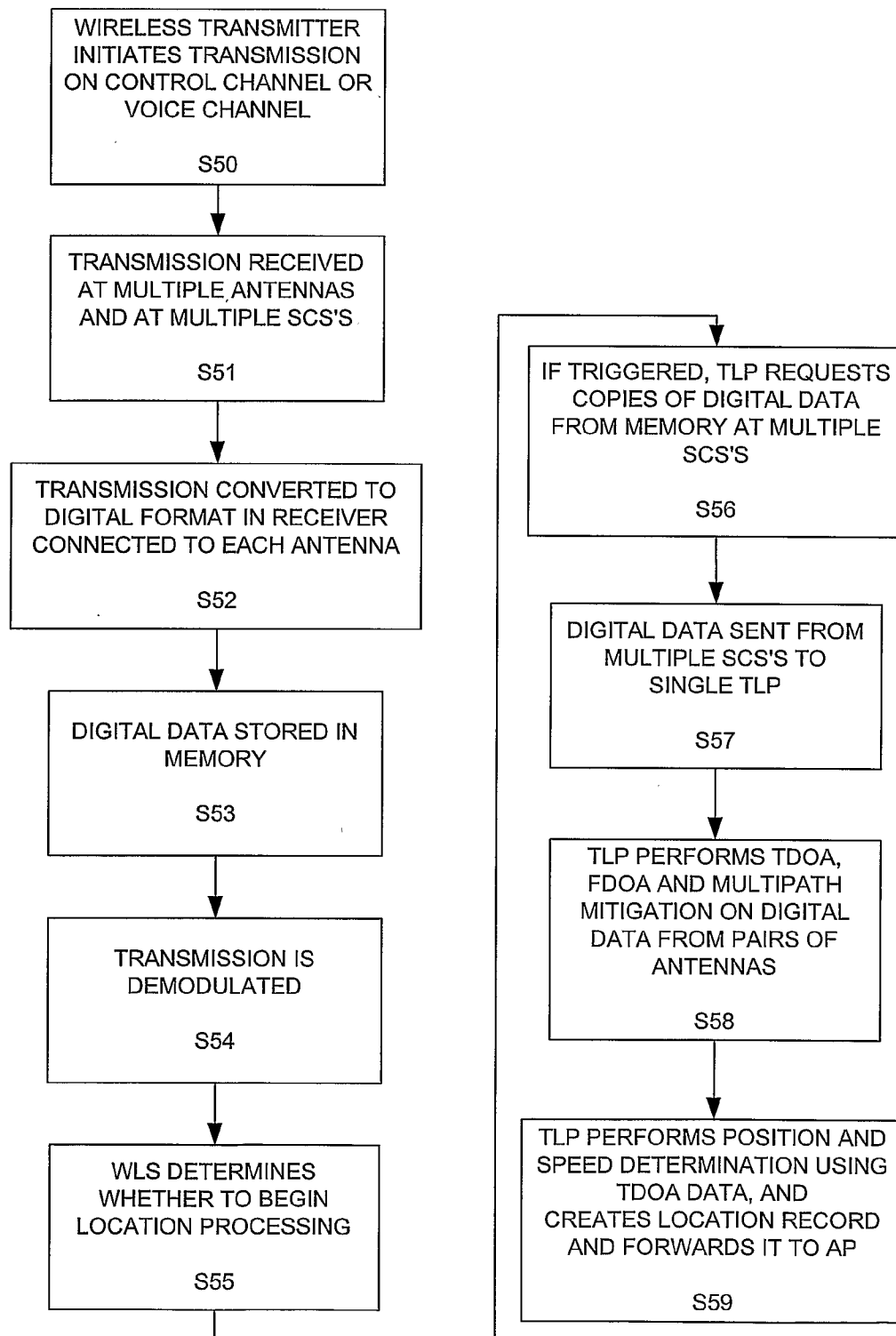


FIGURE 5

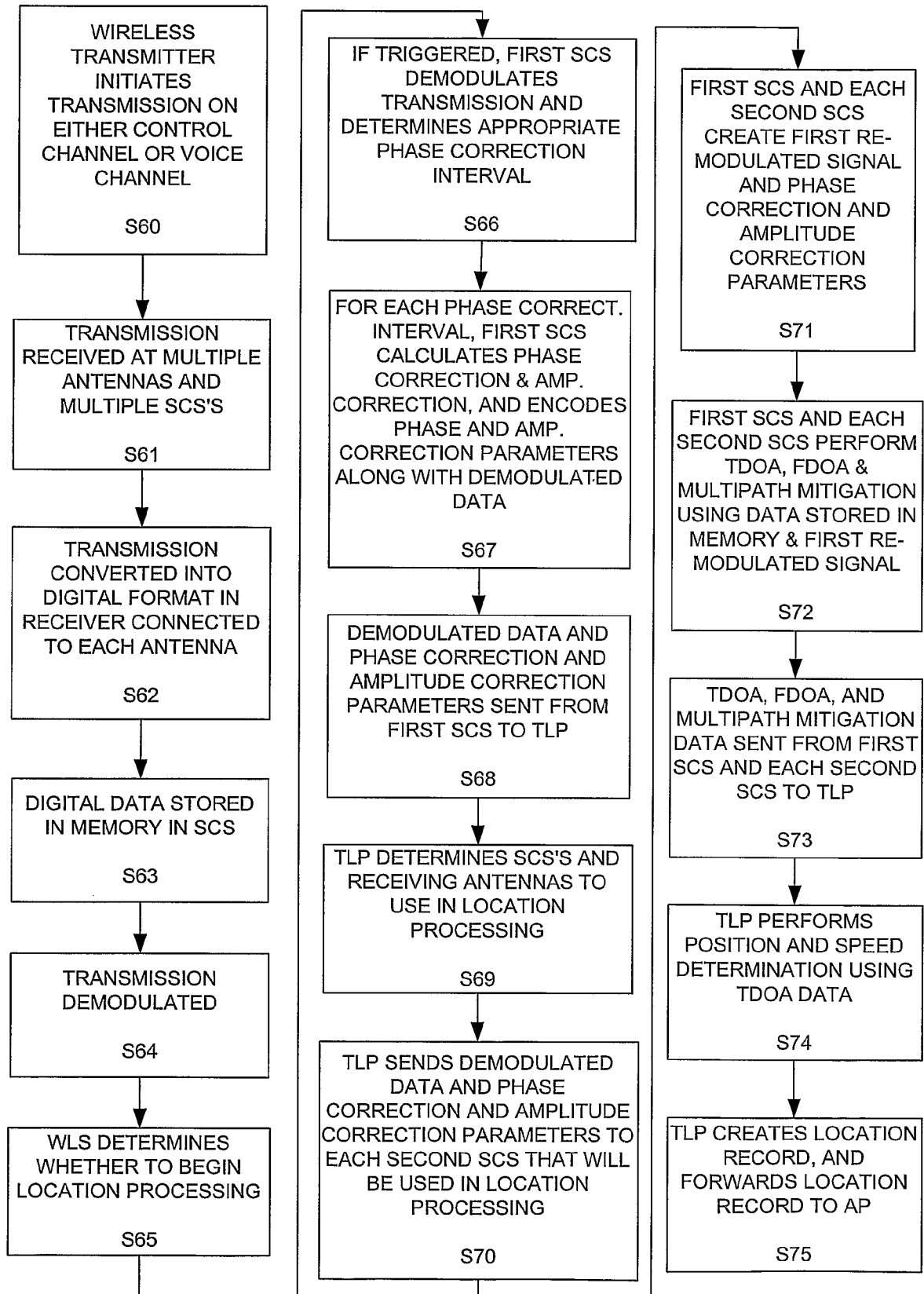
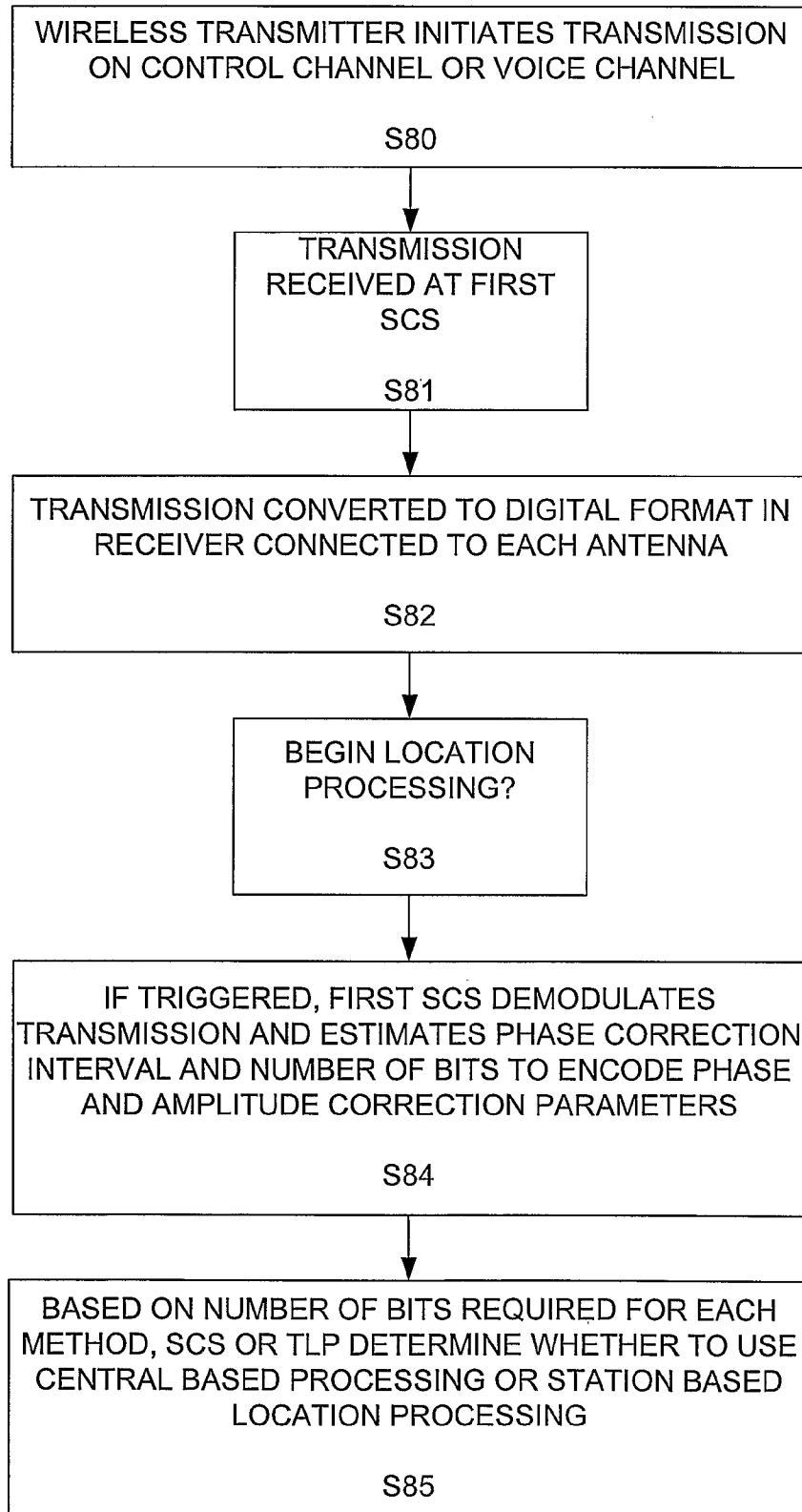


FIGURE 6

**FIGURE 7**

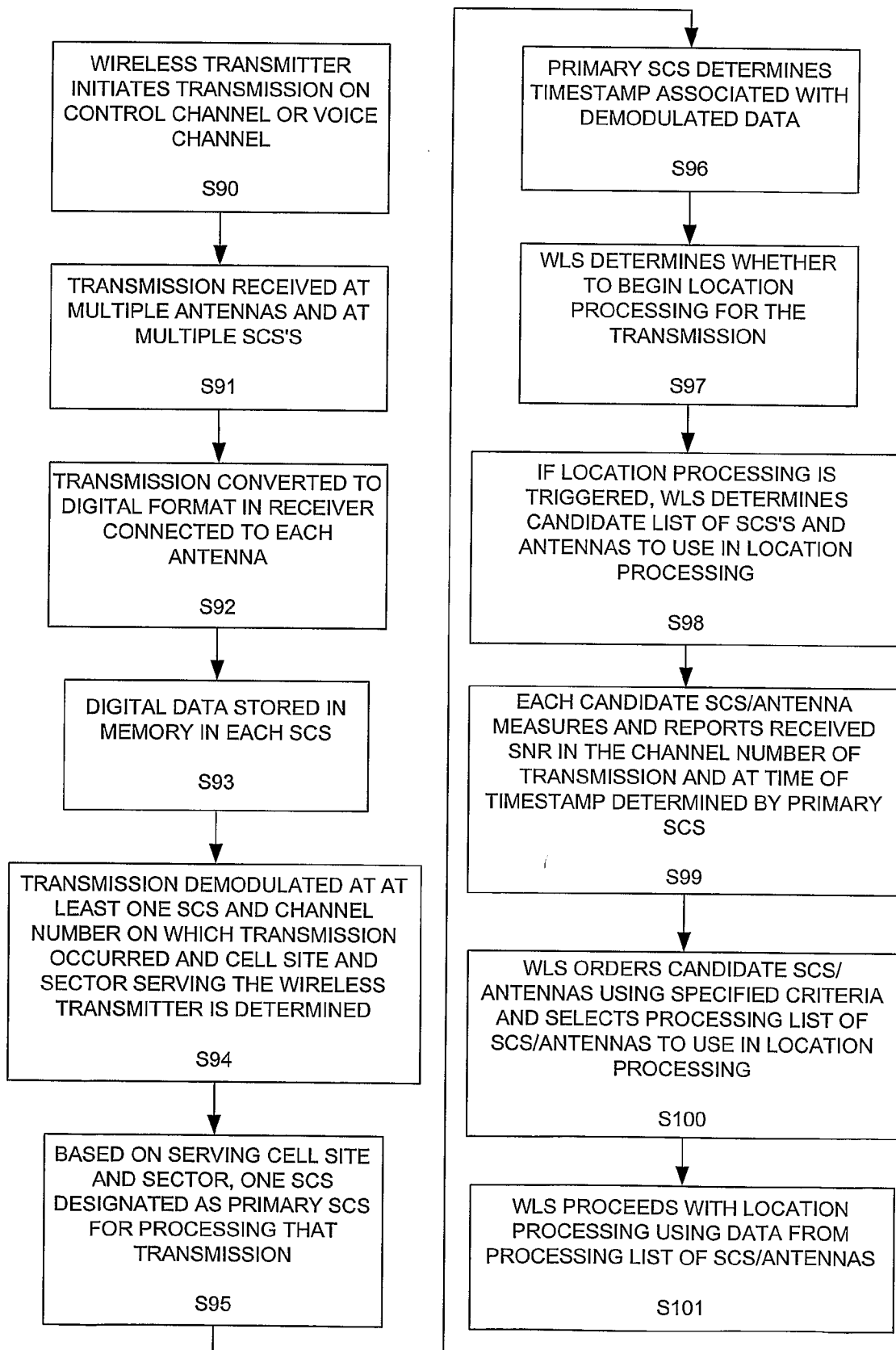


FIGURE 8

23/31

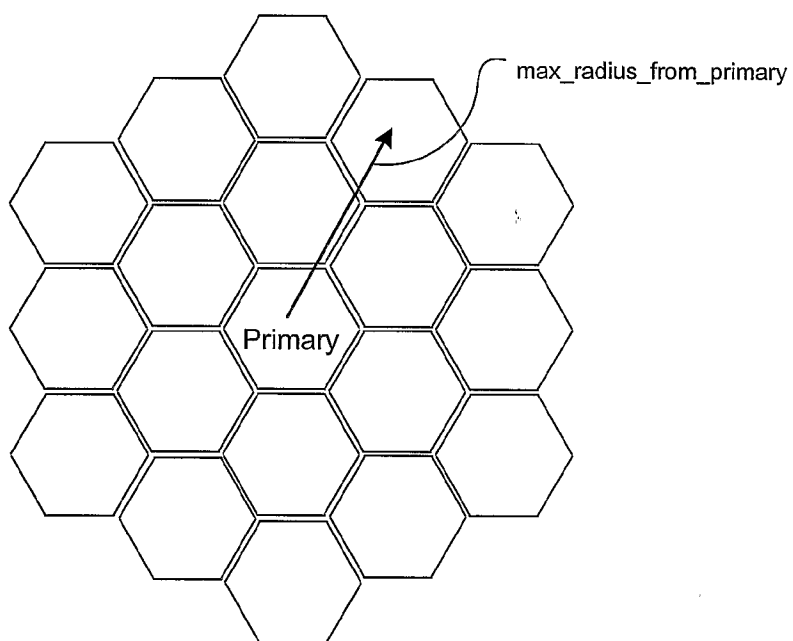
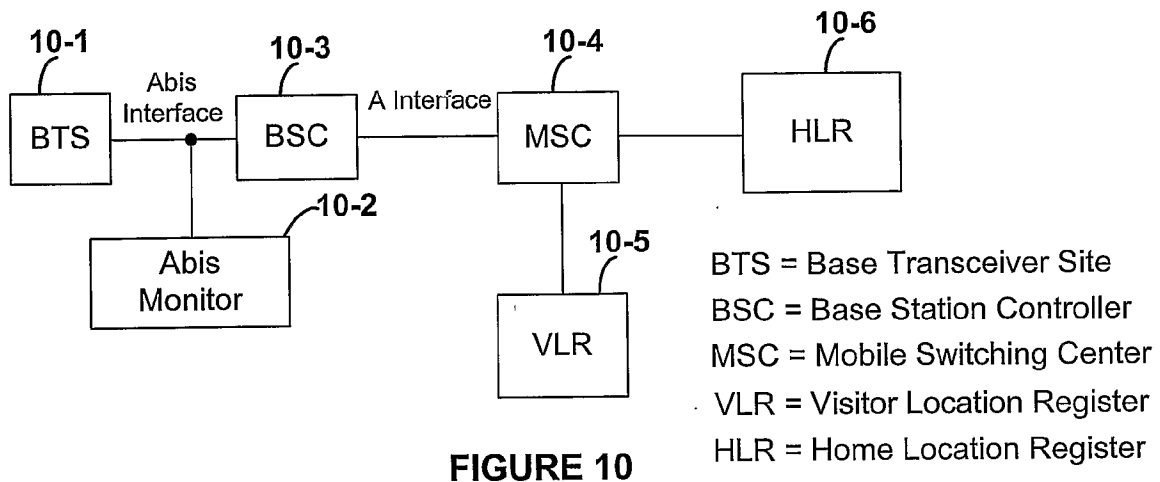
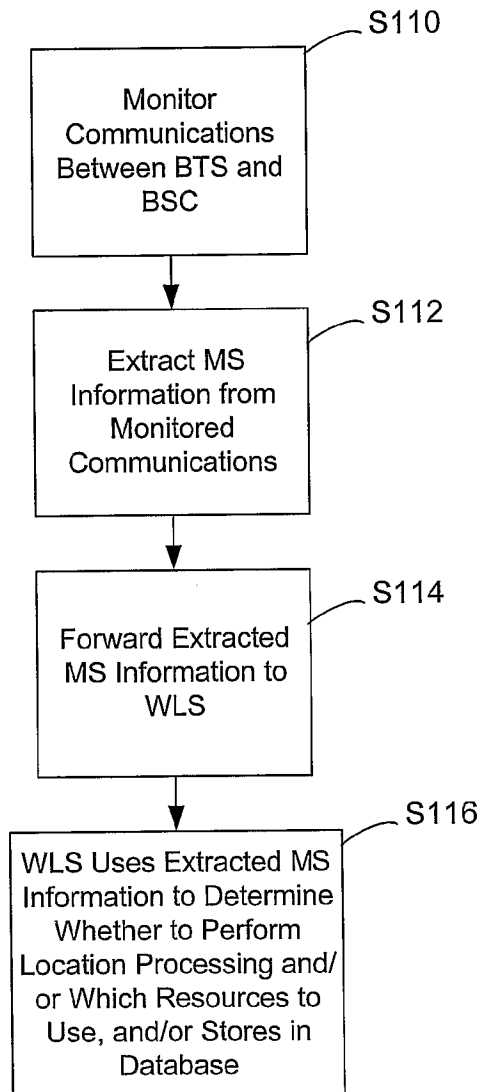
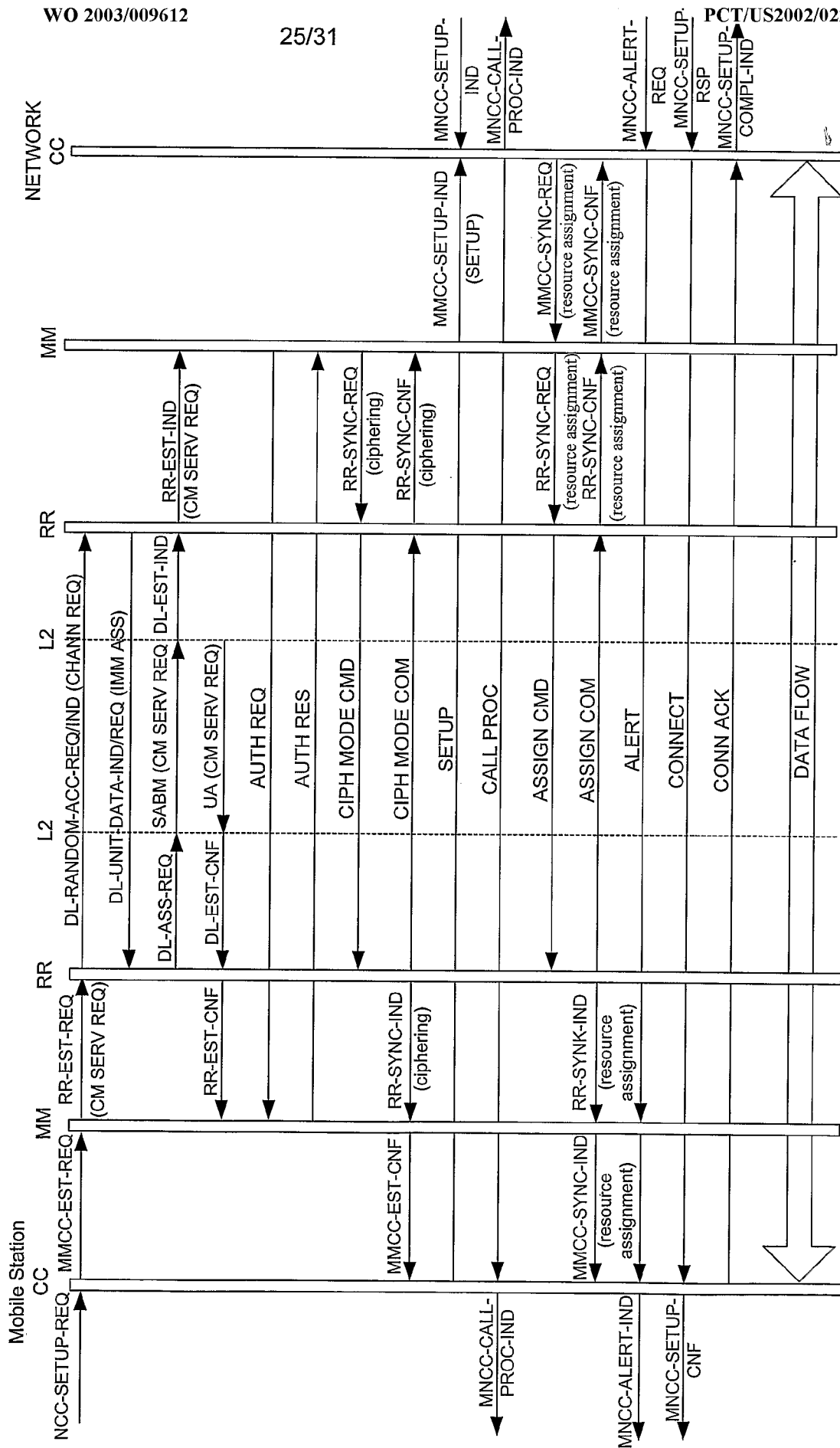


FIGURE 9

24/31

**FIGURE 10****FIGURE 11**



26/31

Tail 7	Synch Sequence 41	Coded Information 36	Tail 7
-----------	-------------------	----------------------	-----------

FIGURE 12B

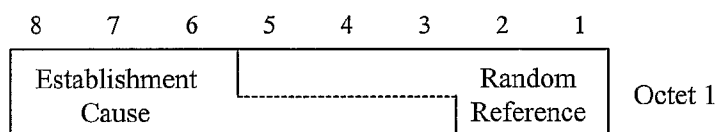


FIGURE 12C

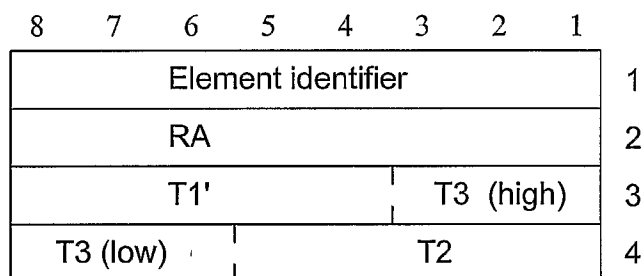


FIGURE 12D

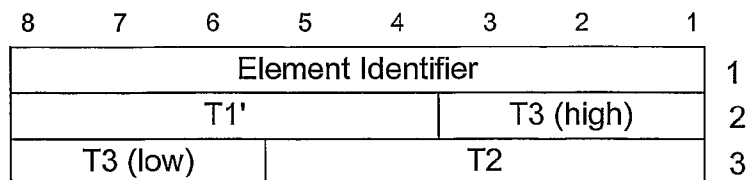


FIGURE 12E

27/31

Information Element	Reference	Presence	Format	Length
Message discriminator	9.1	M	V	1
Message type	9.2	M	V	1
Channel number	9.3.1	M	TV	2
Full Imm. Assign Info	9.3.35	M	TLV	25

FIGURE 12F

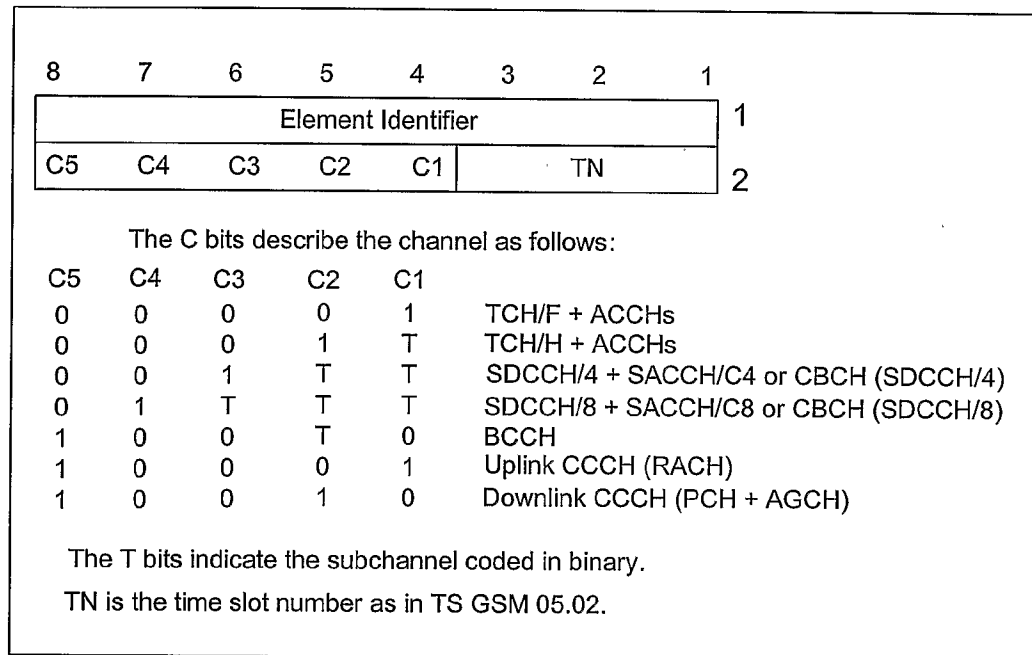


FIGURE 12G

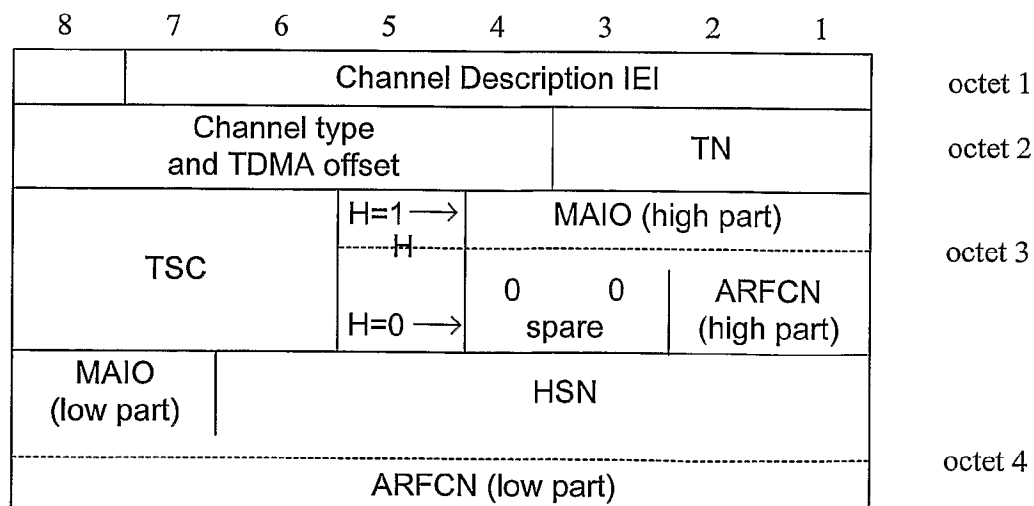
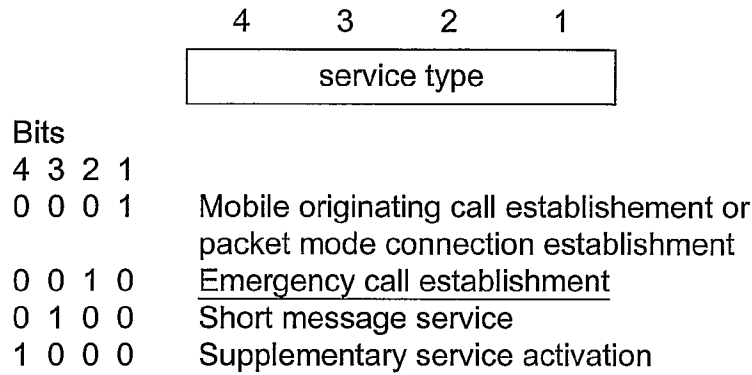


FIGURE 12H



All other values are reserved.

FIGURE 12I (BIT PATTERNS IN CM SERVICE TYPES)

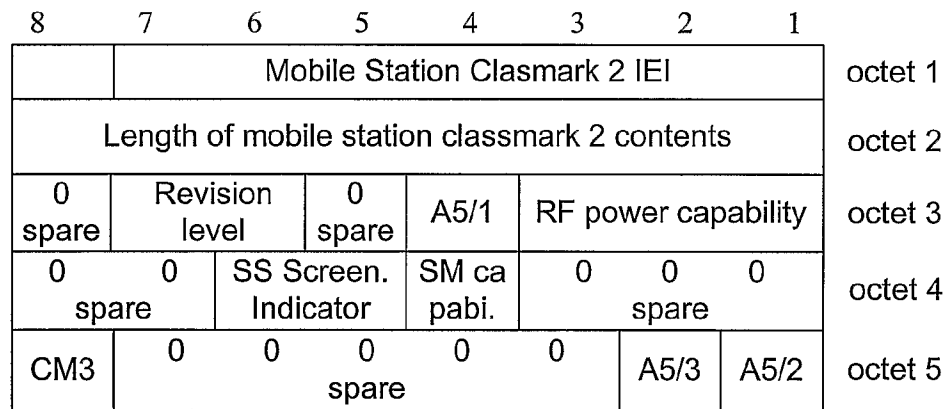


FIGURE 12J (MS CLASSMARK FIELDS IN CM SERVICE REQ.)

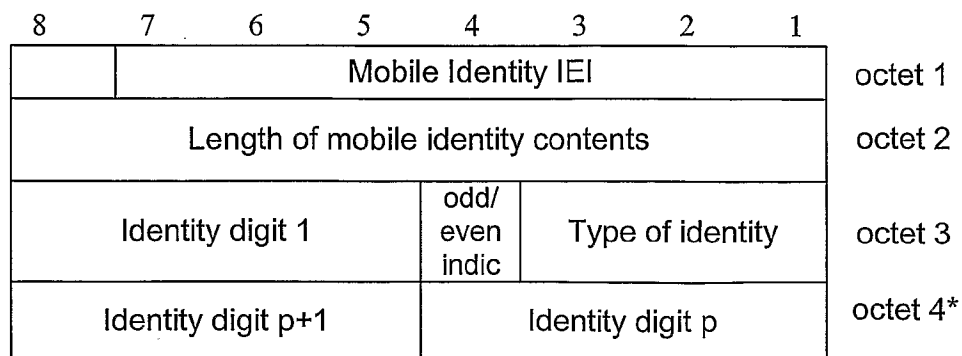


FIGURE 12K (FORMAT OF MOBILE ID FIELDS)

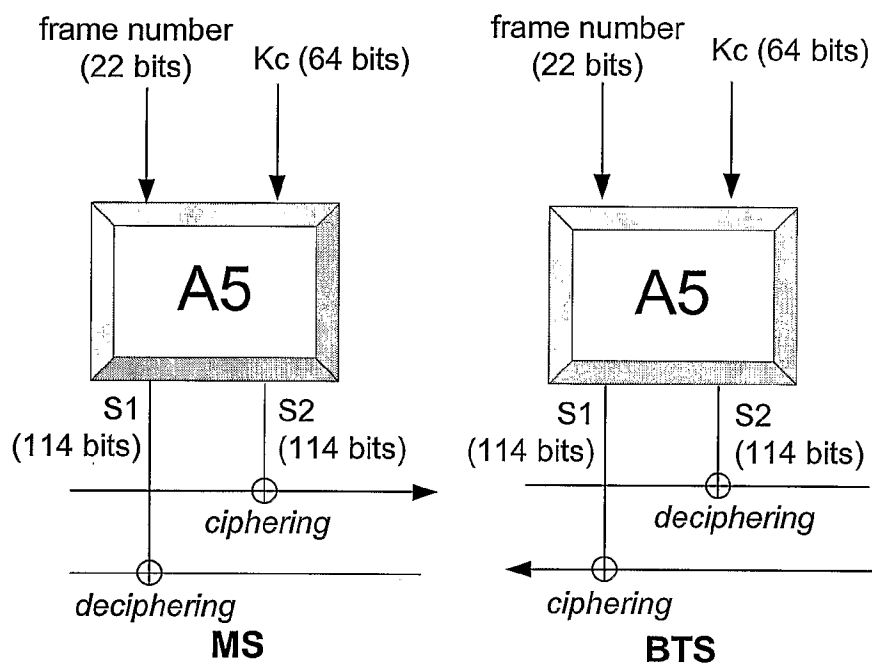


FIGURE 12L

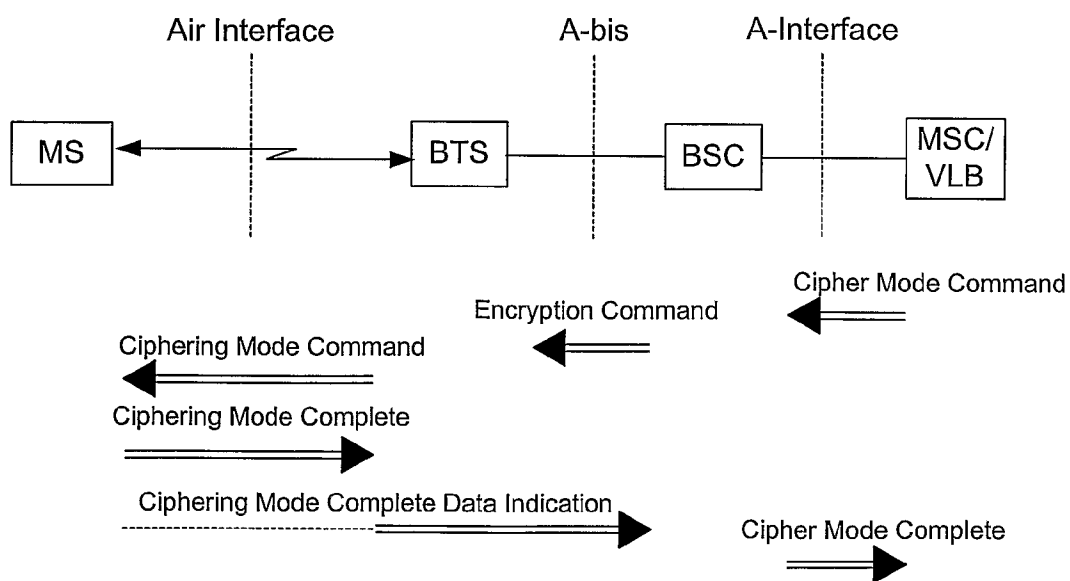


FIGURE 12M

8	7	6	5	4	3	2	1	
Element identifier								1
Length								2
Algorithm identifier								3
Key								4
								n

FIGURE 12N

8	7	6	5	4	3	2	1	
Called party BCD number IEI							octet 1	
Length of called party BCD number contents							octet 2	
1 ext	type of number			Numbering plan identification			octet 3	
Number digit 2			Number digit 1			octet 4*		
Number digit 4			Number digit 3			octet 5*		
Note 2)						:		
						:		

FIGURE 12O

31/31

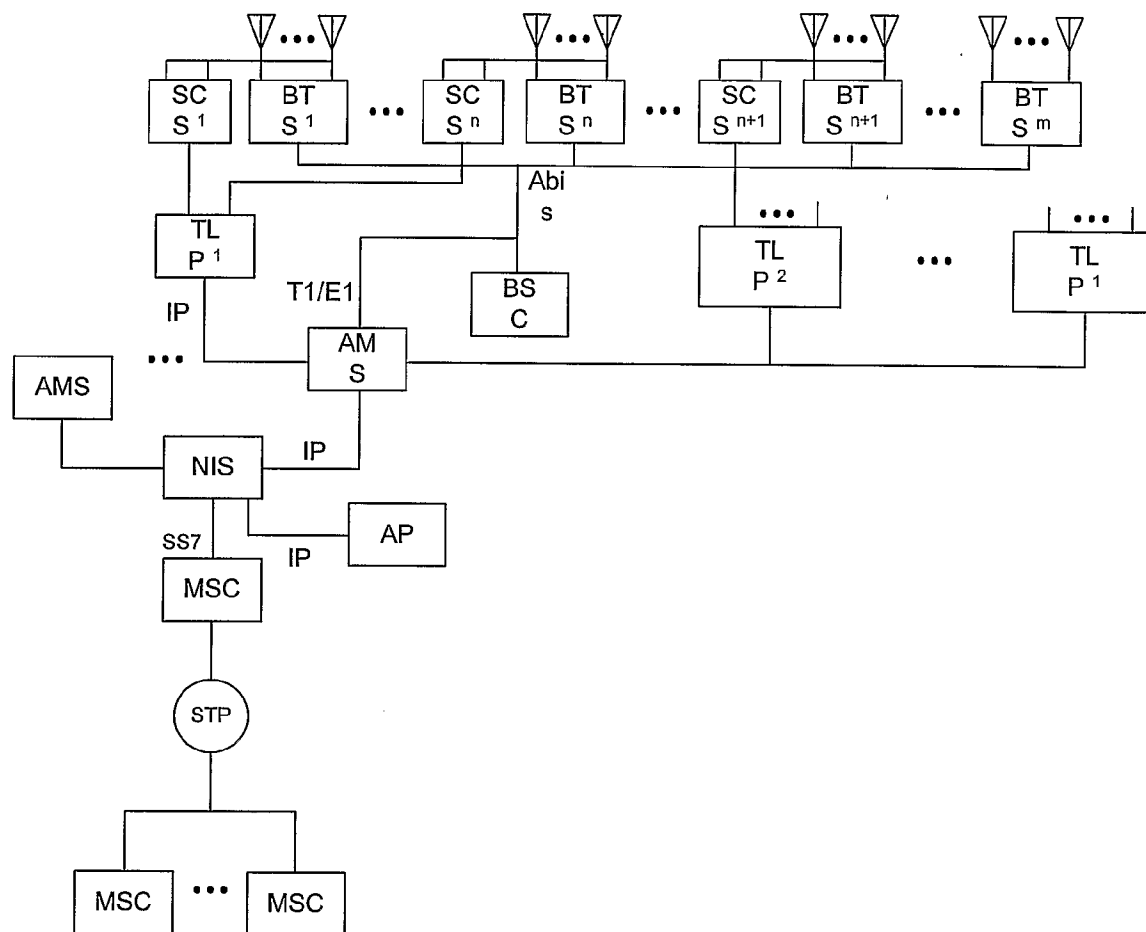


FIGURE 12P

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/22390

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20
US CL : 455/456, 560

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/456, 560, 561, 422; 370/310, 328

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,061,565 A (INNES et al.) 09 May 2000 (09.05.2000), columns 3-5.	1, 4-6, 14, 24
---		-----
Y		2-3, 7-13, 15-23, 25-33
Y	US 5,884,175 A (SCHIEFER et al.) 16 March 1999 (16.03.1999), column 19 lines 3-30.	2-3, 7-13, 15-23, 25-33
A,E	US 6,430,397 B1 (WILLRETT) 06 August 2002 (06.08.2002), columns 2-3.	1-33
A	US 6,088,587 A (ABBADESSA) 11 July 2000 (11.07.2000), columns 5-6, column 8 lines 38-67, column 14 lines 30-67, column 15 line 59 to column 16 line 8.	1-33

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

04 December 2002 (04.12.2002)

Date of mailing of the international search report

19 DEC 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Nguyen T Va

Telephone No. (703) 305-3900